Seri Internet dan Hak Asasi Manusia

PERLINDUNGAN DATA PRIBADI DI INDONESIA

Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia

Penulis:

Wahyudi Djafar
Bernhard Ruben Fritz Sumigar
Blandina Lintang Setianti

ELSAM
LEMBAGA STUDI & ADVOKASI MASYARAKAT

ELSAM
LEMBAGA STUDI & ADVOKASI MASYARAKAT

PERLINDUNGAN DATA PRIBADI

Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia

Penulis:

Wahyudi Djafar
Bernhard Ruben Fritz Sumigar
Blandina Lintang Setianti

Lembaga Studi dan Advokasi Masyarakat (ELSAM)
2016

PERLINDUNGAN DATA PRIBADI

Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia

Penulis:

Wahyudi Djafar
Bernhard Ruben Fritz Sumigar
Blandina Lintang Setianti

Pertama kali dipublikasikan dalam bahasa Indonesia oleh:
Lembaga Studi dan Advokasi Masyarakat (ELSAM)

Semua penerbitan ELSAM didedikasikan kepada para korban pelanggaran hak asasi manusia selain sebagai bagian dari upaya pemajuan dan perlindungan hak asasi manusia di Indonesia.

Except where otherwise noted, content on this report is licensed under a Creative Commons Attribution 3.0 License. Some rights reserved.

DAFTAR ISI

Daftar Isi ..... **iii**
Daftar Tabel ..... **v**

A. PENDAHULUAN **1**

B. PENGERTIAN ATAS KONSEP PERLINDUNGAN DATA PRIBADI **3**

C. PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ATAS PRIVASI **5**

D. MODEL REGULASI PERLINDUNGAN DATA PRIBADI **8**
D.1. Model perlindungan data pribadi: praktik di Eropa, OECD dan APEC 8
D.2. Praktik perlindungan data pribadi di beberapa negara 10
D.3. Cakupan perlindungan data pribadi 25
D.4. Pengawasan terhadap perlindungan data pribadi 27
D.5. Mekanisme pemulihan yang disediakan jika terjadi pelanggaran 28

E. GAMBARAN UMUM REGULASI PERLINDUNGAN DATA PRIBADI DI INDONESIA **28**
E.1. Jaminan konstitusi perlindungan data pribadi 29
E.2. Jaminan perlindungan data pribadi dalam peraturan perundang-undangan 29
E.3. Perkembangan pembangunan instrumen hukum dalam melindungi data pribadi di Indonesia 52

F. BENTUK-BENTUK PELANGGARAN TERHADAP KERAHASIAAN DATA PRIBADI .. **55**

G. USULAN PELEMBAGAAN PERLINDUNGAN DATA PRIBADI DI INDONESIA **58**
G.1. Pembentukan undang-undang tentang perlindungan data pribadi 58
G.2. Pendirian badan pengawasan tentang perlindungan data pribadi 62

H. PENUTUP **66**

Daftar Pustaka **67**
Profil ELSAM **75**

DAFTAR TABEL

Tabel 1
Prinsip-Prinsip Perlindungan Data Pribadi di Uni Eropa 8

Tabel 2
Perbandingan Perlindungan Data Pribadi di Beberapa Negara 24

Tabel 3
Perbandingan Pengaturan terkait Data Pribadi dalam Sejumlah Peraturan Perundang-Undangan di Indonesia 50

Tabel 4
Perbandingan Prinsip Pengolahan, Pembukaan Data dan Akuntabilitas 59

Tabel 5
Perbandingan Institusi Pengawas Berdasarkan Peraturan Perundang-Undangan yang Berlaku di Indonesia 63

BHINNEKA TUNGGAL IKA

A. PENDAHULUAN

Meningkatnya pemanfaatan teknologi internet, selain membuka banyak kesempatan dan peluang pengembangan, termasuk kemudahan dalam pertukaran informasi, pada sisi lain juga telah membuka kerawanan baru terjadinya intervensi terhadap privasi. Peredaran data dalam format digital yang tidak lagi mengenal batas ruang dan teritorial menjadikan semakin mudahnya data-data pribadi seseorang terpapar atau dipindahtangankan secara semena-mena, tanpa kontrol dari pemilik data. Beberapa kasus terkait kebocoran data pribadi seseorang marak ditemukan. Misalnya maraknya promosi produk, mulai dari properti, asuransi, fasilitas pinjaman, dan kartu kredit. Tidak sedikit pula kasus pelanggaran terhadap privasi, terutama data pribadi yang berbuntut pada aksi penipuan. Padahal konsumen sama sekali belum pernah menyerahkan data pribadinya pada produsen produk bersangkutan. Ketidakjelasan pelaku pembocoran atau jual beli data pribadi serta ketidakjelasan mekanisme hukum yang disediakan oleh undang-undang, menjadikan sulitnya komplain atas kerugian yang diderita. Oleh karenanya wacana penguatan perlindungan data pribadi, termasuk mekanismenya, menjadi sangat penting untuk dilaksanakan.

Namun demikian, meski permasalahan intrusi data pribadi telah menjadi permasalahan aktual dan nyata, isu pelanggaran privasi belum menjadi isu populer di kalangan masyarakat Indonesia. Padahal sebagai salah satu negara dengan pengguna aktif internet terbesar di dunia, sudah seharusnya publik didorong memiliki kesadaran lebih akan hak privasinya. Faktanya memang, mayoritas publik di Indonesia belum menjadikan data pribadi sebagai bagian dari properti dan hak asasi manusia yang wajib dilindungi, sehingga *acapkali* kita temukan seseorang yang tanpa sadar mengumbar privasinya dengan sembarangan, termasuk data-data pribadi mengenai dirinya.

Konstitusi Indonesia sendiri sesungguhnya telah secara khusus mengatur jaminan perlindungan hak atas privasi warga negara, sebagaimana ditegaskan Pasal 28 G ayat (1) UUD 1945. Penegasan serupa juga muncul di dalam ketentuan Pasal 29 UU No. 39 Tahun 1999 tentang Hak Asasi Manusia, termasuk juga Indonesia telah meratifikasi Kovenan Internasional Hak-Hak Sipil dan Politik atau *International Covenant on Civil and Political Rights* (ICCPR). Sayangnya, jaminan konstitusional tersebut belum terejawantahkan dengan baik pada tingkat peraturan perundang-undangan. Meski kalau kita lakukan identifikasi dengan seksama, sedikitnya telah ada 30 undang-undang di Indonesia, yang materinya memiliki singgungan atau keterkaitan dengan pentingnya perlindungan data pribadi warga negara. Dalam praktiknya, pemindahtanganan data pribadi seseorang tanpa sepengetahuan dari pemilik data tetap marak terjadi, khususnya yang diduga dilakukan oleh pihak-pihak yang melakukan perekaman dan penyimpanan data pribadi, baik yang dilakukan oleh institusi pemerintah maupun swasta.

Dalam konteks perekonomian global, perlindungan data pribadi sebenarnya telah menjadi instrumen penting untuk melakukan perdagangan internasional. Jaminan perlindungan tersebut menjadi kebutuhan mitra kerjasama ekonomi internasional, seperti *Organisation for Economic Cooperation and Development* (OECD), *Asia-Pacific Economic Cooperation* (APEC) dan *Economic Community for West African States* (ECOWAS).[1] Mereka bahkan pada akhirnya

[1] Graham Greenleaf, "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories", 23 *J.L.I.S.* 1, (2014) hal.17-19 [Greenleaf 'Sheherezade'].

membentuk instrumen khusus demi terlindunginya data pribadi dalam melaksanakan transaksi internasional. Indonesia, sebagai negara strategis dalam perdagangan internasional, memiliki pretensi untuk memiliki peraturan perlindungan data pribadi yang memadai sesuai dengan standar internasional. Kendati faktanya, meski menjadi bagian dari APEC, sampai dengan saat ini Indonesia tidak kunjung memiliki aturan khusus mengenai perlindungan data pribadi. Selain itu, bila kita bandingkan dengan negara-negara lainnya, khususnya di kawasan Asia Tenggara, yang tergabung dalam ASEAN, Indonesia menjadi negara yang paling tertinggal dalam menyiapkan perangkat perlindungan data privasi bagi warganya, baik dari segi waktu maupun variasi perlindungannya.

Selain dari segi ekonomi, perlindungan data pribadi juga harus dipandang sebagai tantangan dalam perlindungan hak asasi manusia (HAM). Perlindungan data mengisyaratkan bahwa individu berhak untuk menentukan apakah mereka akan membagi atau bertukar data pribadi mereka atau tidak. Selain itu, individu berhak pula menentukan syarat pelaksanaan pemindahtanganan data tersebut. Hal ini menjadi penting, mengingat kasus pelanggaran terhadap hak atas privasi, terutama data pribadi, sangat marak terjadi.

Dalam laporannya, Pelapor Khusus Perserikatan Bangsa-Bangsa (PBB) untuk Pemajuan dan Perlindungan Hak atas Kebebasan Berpendapat dan Berekspresi (*United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*), Frank La Rue, menegaskan perlunya setiap negara memiliki undang-undang yang secara jelas menggambarkan mengenai pembatasan hak atas privasi dari individu dalam situasi tertentu. Aturan mengenai hal ini harus didasari dengan sebuah keputusan khusus yang dilakukan negara sesuai dengan hukum.[2] Dewan HAM PBB sendiri dalam perkembangannya telah membentuk Pelapor Khusus untuk Hak Atas Privasi dalam sesi persidangan ke-28 Dewan HAM pada 24 Maret 2015, melalui Resolusi 28/16. Resolusi ini merupakan tindak lanjut dari Resolusi Majelis Umum PBB 68/167 tentang Hak Atas Privasi di Era Digital, yang lebih dulu dikeluarkan pada bulan Desember 2013.

Dalam kerangka itulah Lembaga Studi dan Advokasi Masyarakat (ELSAM) mencoba menginisiasi suatu studi, untuk melihat sejauh mana peluang pelembagaan perlindungan data pribadi dari perspektif hak asasi manusia di Indonesia. Penetrasi pengguna internet yang semakin besar di Indonesia, termasuk makin variatifnya penggunaan teknologi ini dalam pengembangan sistem elektronik, baik dalam konteks perdagangan, perbankan, maupun layanan publik seperti kesehatan, menjadikan semakin pentingnya kehadiran undang-undang perlindungan data pribadi. Studi ini mencoba melihat secara konseptual mengenai perlindungan data pribadi, praktiknya di sejumlah negara, pentingnya bagi perlindungan hak asasi manusia, peta regulasi di Indonesia, serta rekomendasi pelembagaan kebijakannya ke depan, dengan mengacu pada standar dan prinsip hak asasi manusia.

[2] UN Doc.A/HRC/17/27 (2011) para.58-59.

B. PENGERTIAN ATAS KONSEP PERLINDUNGAN DATA PRIBADI

Pemahaman akan perlindungan data pribadi tentunya tidak terlepas dari pemaknaan terhadap "data" yang dapat diklasifikasikan sebagai "data pribadi", serta bagaimana bentuk perlindungan yang dapat diberikan terhadap data pribadi yang bersangkutan.

Secara harafiah data merupakan bentuk jamak dari kata "*datum*" yang dalam bahasa Latin bermakna sebagai bagian informasi[3] atau dengan kata lain data dapat dipahami sebagai kumpulan dari *datum-datum* yang melahirkan suatu informasi. Data harus pula memuat sekelompok fakta dalam bentuk simbol-simbol [seperti alfabet, angka, citra maupun simbol khusus lainnya][4] yang merepresentasikan ide, objek, kondisi atau situasi, yang dapat disusun untuk diolah dalam bentuk struktur data, struktur *file*, dan *database*.[5] Seiring dengan berkembangnya cara pengumpulan suatu data, maka beragam variabel jenis data, *inter alia*, data primer-sekunder, data kualitatif-kuantitatif, hingga data pribadi, lahir dengan sendirinya.

Khusus untuk konteks data pribadi, dewasa ini tiap-tiap negara di dunia menggunakan peristilahan yang berbeda antara "informasi pribadi" dan "data pribadi". Akan tetapi secara substantif kedua istilah tersebut mempunyai pengertian yang hampir sama, sehingga kedua istilah tersebut sering digunakan bergantian.[6] Di Amerika Serikat, Kanada dan Australia menggunakan istilah informasi pribadi(*personally identifiable information (PII)*), sedangkan negara-negara di Eropa dan Indonesia[7] menggunakan istilah data pribadi (*personal data*). Sehingga, untuk keperluan tulisan ini, penulis akan merujuk kepada istilah data pribadi.

Lebih jauh, tidak hanya sekedar penggunaan istilah saja yang berbeda, penafsiran terhadap terminologi data pribadi pun bertolak belakang antara sistem hukum di Amerika Serikat dengan yang ada di Eropa. Amerika Serikat tidak memiliki instrumen khusus yang secara rigid menafsirkan makna data pribadi, akan tetapi mereka memberikan tiga peluang pendekatan untuk menguraikan istilah tersebut, yakni dengan memakai pendekatan tautologikal (*tautological approach*), pendekatan non-publik (*non-public approach*) dan pendekatan khusus (*specific type approach*).[8]

Sementara itu, kawasan Eropa telah memiliki instrumen hukum bernama *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981* (Konvensi 108)[9] dan *Directive 95/46/EC* atau yang dikenal dengan sebutan *European Union Data Protection Directive 1995* (*DP Directive*),[10] yang pada butir Pasal 2 huruf (a) kedua instrumen ini menguraikan data pribadi sebagai "*information relating to an identified or identifiable*

---

[3] Bryan A. Garner (ed.), *Black's Law Dictionary*, 8th Edition, (St. Paul: West Pub. Co., 2004) hal.423.

[4] P. Beynon-Davies, *Information Systems: An Introduction to Informatics in Organisations*, (Basingstoke: Palgrave Macmillan, 2002).

[5] Purwanto, *Penelitian tentang Perlindungan Hukum Data Digital*, (Jakarta: BPHN Departemen Hukum dan HAM, 2007) hal.14 [Purwanto].

[6] Shinta Dewi Rosadi, *CyberLaw: Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasional*, (Bandung: Widya Padjadjaran, 2009) hal.71 [Rosadi].

[7] Lihat Pasal 26 ayat (1) UU ITE.

[8] Untuk uraian terhadap ketiga pendekatan ini lihat Paul M. Schwartz dan Daniel J. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", 86 *N.Y.U. L. Rev.* 1814, (2011) hal.1828-1836 [Schwartz dan Solove (2011)].

[9] E.T.S. No.108/1981.

[10] O.J. L. 281, 23 November 1995, hal.31–50 [*DP Directive*].

natural person". Hal ini sejalan dengan penafsiran OECD yang melihat data pribadi sebagai suatu informasi yang teridentifikasi atau dapat diidentifikasi menyangkut pribadi seseorang.[11]

Konsepsi data pribadi yang diadopsi oleh Uni Eropa dan OECD ini kemudian dijadikan rujukan bagi Indonesia dalam menyusun rumusan pengertian data pribadi pada ketentuan Pasal 1 ayat (1) Rancangan Undang-Undang tentang Perlindungan Data Pribadi (RUU PDP) berikut ini:[12]

> "*Data pribadi adalah setiap data yang terindetifikasi dan/atau dapat diidentifikasi, baik secara langsung maupun tidak langsung melalui elektronik atau non elektronik.*"

Meskipun mengacu kepada kedua instrumen tersebut di atas, nyatanya materi muatan terkait dengan konsepsi data pribadi dalam RUU PDP memiliki perbedaan satu sama lain. Pada RUU PDPterdapatnilai tambah (*added values*) yang tidak ditemui dalam instrumen hukum di Uni Eropa dan OECD. Ketentuan RUU PDP secara tegas memuat klausula "*baik secara langsung maupun tidak langsung*" serta memberikan batasan data pribadi baik yang terbentuk "*melalui* [sarana]*elektronik atau non elektronik*". Pemahaman secara komprehensif terhadap nilai tambah ini mutlak diperlukan agar pemaknaan data pribadi itu menjadi tidak kabur (*obscure*).

Selain dalam RUU PDP, konsepsi data pribadi ditafsirkan berbeda oleh Pasal 1 ayat (27) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Peraturan tersebut memaknai data sebagai data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenarannya serta dilindungi kerahasiaannya.

Dalam hal perlindungan terhadap data pribadi, setidaknya dikenal dua metode untuk melindungi suatu data pribadi, yakni, pertama dengan melakukan pengamanan terhadap fisik data pribadi itu sendiri.[13] Selain itu, metode kedua yang dapat ditempuh untuk melindungi data pribadi adalah melalui sisi regulasi yang bertujuan untuk memberi jaminan privasi terhadap penggunaan data pribadi tersebut.[14]

Sehubungan dengan metode yangkedua, sejarah mencatat bahwa perlindungan data pribadi atau dikenal dengan istilah "*data protection*" mulai pertama kali digunakan dalam undang-undang di beberapa negara di daratan Eropa, yaitu Jerman, Swedia dan Prancis pada era tahun 1970-an.[15] Perlindungan data pribadi di sejumlah negara inisepenuhnya didasari oleh dorongan untuk menjamin hak atas privasi setiap individu terhadap data tersebut, sejalan dengan berkembangnya teknologi informasi dan komunikasi, kemudian cakupan pengaturannya merambah hingga ke aspek administrasi publik di sana.

---

[11] *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, (1980) para.1(b) [*OECD Guidelines*].

[12] Direktorat Jenderal IKP, Kementerian Komunikasi dan Informasi, dan Cyberlaw Centre Fakultas Hukum, Universitas Padjadjaran Bandung, *Naskah Akademik Rancangan Undang-Undang tentang Perlindungan Data Pribadi*, (2014) hal.32 [Naskah Akademik RUU PDP].

[13] Purwanto, *Op.Cit.*, hal.13.

[14] Nancy Yue Liu, *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics*, (Oxon: Routledge, 2012) hal.21.

[15] Rosadi, *Op.Cit.*, hal.37.

C. PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ATAS PRIVASI

Konsep perlindungan data sering diperlakukan sebagai bagian dari perlindungan terhadap hak atas privasi. Perlindungan data pada dasarnya dapat berhubungan secara khusus dengan privasi seperti yang dikemukakan oleh Alan Westin yang untuk pertama kalinya mendefinisikan data privasi atau "*information privacy*" sebagai hak individu, kelompok atau lembaga untuk menentukan sendiri mengenai kapan, bagaimana dan sampai sejauh mana informasi tentang mereka dikomunikasikan atau tidak kepada pihak lain.[16]

Definisi yang dikemukakan oleh Westin tersebut, kemudian dikembangkan oleh para pakar hukum lainnya, seperti Arthur Miller yang mendeskripsikan data privasi sebagai kemampuan individu untuk mengontrol penyebaran informasi terkait dengan dirinya sendiri,[17] sebab melalui kemajuan teknologi maka informasi pribadi seseorang dapat diakses, diproses, dikumpulkan dan dimanipulasi secara cepat dan murah. Oleh karenanya, Westin memandang bahwa hak atas privasi ini tidak bersifat absolut karena ada kewajiban sosial yang harus diperhatikan yang sama pentingnya dengan privasi.[18]

Konsep hak atas privasi juga diperkukuh pula oleh tulisan Warren dan Brandeis yang menegaskan konsep privasi sebagai sebuah hak bagi setiap individu untuk menikmati kehidupannya atau disebut dengan "*the right to be alone*"; sebagai suatu hak yang harus dilindungi oleh hukum.[19] Pemahaman konsep privasi sebagai suatu hak yang diutarakan oleh Warren dan Brandeis ini, kemudian mendorong pemuatan konsep hak atas privasi dalam Pasal 12 Deklarasi Umum Hak Asasi Manusia yang menyatakan:

> "*Tidak seorangpun dapat diganggu dengan sewenang-wenang urusan pribadi, keluarga, rumah tangga atau hubungan surat-menyuratnya, juga tak diperkenankan pelanggaran atas kehormatan dan nama baiknya. Setiap orang berhak mendapat perlindungan hukum terhadap gangguan atau pelanggaran seperti itu.*"

Berdasarkan Deklarasi ini, maka privasi dapat dianggap sebagai suatu kondisi di mana setiap individu harus memiliki otonomi, kebebasan, termasuk kebebasan berinteraksi, dalam sebuah "ruang privat" dengan atau tanpa orang lain, bebas dari intervensi negara dan intervensi yang berlebihan dari individu lainnya. Ketentuan yang singkat dan lugas ini lalu dipertegas oleh ketentuan dalam Pasal 17 ICCPR yang mengatur:

> "*(1) Tidak boleh seorangpun yang dapat secara sewenang-wenang atau secara tidak sah dicampuri masalah-masalah pribadinya, keluarganya, rumah atau hubungan surat-menyuratnya, atau secara tidak sah diserang kehormatan dan nama baiknya.*
> *(2) Setiap orang berhak atas perlindungan hukum terhadap campur tangan atau serangan seperti tersebut di atas.*"

---

[16] Alan F. Westin, *Privacy and Freedom*, (London: Atheneum, 1967) hal.7 [Westin].
[17] Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers*, (Ann Arbor: University of Michigan Press, 1971) hal.25.
[18] Westin, *Op.Cit.*, hal.7.
[19] Samuel Warren dan Louis D. Brandeis, "The Right to Privacy", 4 *Harv. L. Rev.* 5 (1890) hal.1.

Evolusi hak atas privasi dalam kerangka Pasal 17 ICCPR ini kemudian di pandang oleh Manfred Nowak dapat merambah hingga aspek hak atas akses dan kontrol data pribadi seseorang.[20] Pada akhirnya, pandangan Nowak tersebut pun diamini oleh HRC yang secara tegas mengafirmasi hal ini dalam Komentar Umum 16 ICCPR yang berbunyi:[21]

> "*Pengumpulan dan penyimpanan informasi pribadi di komputer, bank data dan alat mekanik lainnya, baik oleh pihak berwenang publik atau individu-individu atau badan-badan, harus diatur oleh hukum. Langkah-langkah yang efektif harus diambil oleh negara-negara guna menjamin bahwa informasi yang berkaitan dengan kehidupan pribadi seseorang tidak jatuh ke tangan orang-orang yang tidak memiliki kewenangan secara hukum untuk menerima, memproses dan menggunakannya, dan tidak boleh digunakan untuk tujuan-tujuan yang tidak sesuai dengan ICCPR. Guna mendapatkan perlindungan yang efektif bagi kehidupan pribadinya, setiap individu harus memiliki hak untuk menentukan data-data pribadi apa dan untuk tujuan apa yang akan disimpan dalam rekaman data otomatis. Jika rekaman data tersebut memuat data pribadi yang tidak benar atau dikumpulkan atau diproses dengan cara yang bertentangan dengan ketentuan-ketentuan hukum, maka setiap individu harus memiliki hak untuk meminta perbaikan atau pemusnahan data tersebut.*"

Seiring dengan pesatnya era digitalisasi pasca terbentuknya Komentar Umum di atas, maka hal ini kemudian mendorong Dewan HAM PBB (*UN Human Rights Council*) untuk pertama kalinya menunjuk Joseph Cannataci dari Malta sebagai Pelapor Khusus PBB untuk Hak atas Privasi (*UN Special Rapporteur on the Right to Privacy*) pada tahun 2015 yang memiliki tiga fungsi pokok, yakni untuk mengidentifikasi tantangan perlindungan hak atas privasi, untuk memajukan prinsip-prinsip dan praktik-praktik terbaik yang ada di tingkat nasional, regional dan internasional, serta untuk memberikan rekomendasi kepada Dewan HAM PBB.[22]

Namun, jauh sebelum penugasan ini diberikan, isu mengenai perlindungan data pribadi dalam kerangka hak atas privasi telah disampaikan oleh Pelapor Khusus Frank La Rue yang mengakui kelemahan perlindungan data pribadi sekarang ini dimotori oleh tidak cukup dan memadainya undang-undang yang ada untuk menjamin hal tersebut di tengah pesatnya era digitalisasi itu sendiri.[23] Penegakan hak atas privasi dalam konteks perlindungan data pribadi ini acap kali menghadapi gangguan yang berpotensi melanggar hak itu sendiri. Mulai dari pengambilan dan pengumpulan data melalui program pemantauan massal (*mass surveillance programme*) yang diikuti retensi terhadap data yang bersangkutan, hingga ancaman kemungkinan data tersebut diambil[24] dapat menimbulkan gangguan terhadap hak atas privasi seseorang.[25]

Hal ini tentunya tak lain dan tak bukan dipengaruhi oleh *status quo* hak atas privasi itu sendiri sebagai suatu hak yang dapat kurangi (*derogable rights*), seperti termaktub dalam Pasal 4 ayat (1) ICCPR. Pengurangan atas penikmatan hak ini sesungguhnya hanya dimungkinkan

---

[20] Manfred Nowak, *U.N. Covenant on Civil and Political Rights CCPR Commentary*, 2nd rev. Ed., (Kehl: N.P. Engel Verlag, 2005) hal.401-402.
[21] UN Doc.CCPR/C/GC/16 (1994) para.10.
[22] *Human Rights Council Resolution 28/16*, UN Doc.A/HRC/RES/28/16 (2015) para.4.
[23] UN Doc.A/HRC/17/27 (2011) para.56.
[24] *Weber and Saravia v. Germany*, No.54934/00, Eur.Ct.H.R. (2006) para.78.
[25] UN Doc.A/HRC/27/37 (2014) para.20.

sepanjang hal tersebut bukanlah suatu bentuk gangguan yang sewenang-wenang (*arbitrary interference*) ataupun gangguan yang melawan hukum (*unlawful interference*).

Menurut Komite HAM PBB (*UN Human Rights Committee/HRC*), konsep 'gangguan yang sewenang-wenang' tidak dapat dipersamakan dengan 'gangguan yang melawan hukum'. Untuk konsep yang terakhir, secara tidak langsung HRC menyatakan bahwa gangguan tidak dimungkinkan, kecuali ditentukan oleh hukum dan harus pula sejalan dengan ketentuan dan tujuan ICCPR itu sendiri.[26] Artinya, segala macam bentuk gangguan di luar hukum yang berlaku dapat dikualifisir sebagai *unlawful interference*.

Sementara itu untuk konsep *arbitrary interference*, hal ini ditafsirkan HRC sebagai suatu bentuk gangguan yang meskipun sah atau dimungkinkan oleh undang-undang, gangguan tersebut haruslah tetap memperhatikan koridor-koridor yang telah ditentukan dalam ICCPR, serta mempertimbangkan aspek kewajarannya (*reasonableness*).[27] Dengan kata lain, agar suatu gangguan tidak diklasifikasikan sebagai suatu hal yang sewenang-wenang, maka ia tetap harus memperhatikan unsur-unsur pembatasan (*limitation*)[28] yang tertuang dalam ICCPR dan instrumen lain yang terkait dengan Kovenan tersebut.

Tidak hanya di tingkat internasional semata, dalam tatanan regional pengakuan perlindungan data pribadi juga diakui sebagai bagian dari hak atas privasi. Di Eropa, Pengadilan HAM Eropa (*European Court of Human Rights*) mengamini perlindungan data pribadi sebagai hal yang fundamental bagi penikmatan dan penghormatan hak atas privasi seseorang sebagaimana diatur dalam Pasal 8 Konvensi HAM Eropa atau*European Convention on Human Rights and Fundamental Freedoms* (ECHR).[29]

Sementara itu di kawasan Amerika, perlindungan data pribadi dalam konteks hak atas privasi dijamin pada Pasal 11 *American Convention on Human Rights*. Khusus untuk konteks Asia Tenggara, pengakuan itu tercermin secara jelas pada Deklarasi HAM ASEAN 2012 (*ASEAN Human Rights Declaration/AHRD*) yang pada butir 21 memuat:

> "*Setiap orang memiliki hak untuk terbebas dari campur tangan yang sewenang-wenang terhadap privasi, keluarga, tempat tinggal, atau yang terkait termasuk data pribadi, atau untuk menyerang kehormatan dan reputasi orang tersebut. Setiap orang berhak atas perlindungan hukum terhadap gangguan atau serangan tersebut.*"

Muatan secara eksplisit terkait perlindungan data pribadi sebagai bentuk khusus dari perlindungan terhadap hak atas privasi ini, menunjukkan perbedaan mencolok antara AHRD dengan instrumen regional di Eropa dan Amerika tersebut di atas yang pada materi muatan pasalnya tidak secara khusus mencantumkan frasa "data pribadi".

[26] UN Doc.CCPR/C/GC/16 (1994) para.3.
[27] *Id.*, para.4.
[28] Penjelasan mengenai unsur-unsur pembatasan ini dapat dilihat dalam Bagian D.3.
[29] Lihat *MK v. France*, No.19522/09, Eur.Ct.H.R. (2013) para.35; *Hannover v. Germany*, No.59320/00, Eur.Ct.H.R. (2004) para.186; *Leander v. Sweden*, No.9248/81, Eur.Ct.H.R. (1987) para.60.

D. MODEL REGULASI PERLINDUNGAN DATA PRIBADI

Pengaturan yang ditujukan sebagai mekanisme perlindungan terhadap data pribadi dalam kerangka pemenuhan hak atas privasi tercermin pada beberapa model regulasi yang dibentuk oleh sejumlah pihak, termasuk organisasi internasional, seperti kawasan Eropa, OECD dan APEC. Tidak hanya itu, beragam model perlindungan data pribadi pada sejumlah negara di dunia juga memperkaya khazanah model regulasi itu sendiri. Berbabagai model regulasi ini menunjukan krusialnya perlindungan data pribadi bagi hak asasi. Model regulasi perlindungan data pribadi juga memuat isu terkait dengan pengawasan terhadap pengelolaan data pribadi yang bersangkutan. Selain itu, mekanisme pemulihan bagi korban pelanggaran hak atas privasi atas data pribadinya, juga menjadi bagian penting dalam pembicaraan ini.

D.1. Model perlindungan data pribadi: praktik di Eropa, OECD dan APEC

Sebagai kawasan yang dipandang paling maju dalam memberikan jaminan perlindungan data pribadi, kawasan Eropa telah memiliki Konvensi 108,*DP Directive*, *Directive 97/66/EC* (*Directive on privacy and telecommunications*)[30] dan *Directive 2002/58/EC* (*Directive on privacy and electronic communications*)[31] yang menjadi payung hukum atas semua pengaturan data pribadi dalam kerangka hak atas privasi yang diakui pada Pasal 8 ECHR dan Pasal 7 Piagam Uni Eropa. Sehubungan dengan hal tersebut, realisasi dari perlindungan data pribadi ini kemudian dijamin dengan lima prinsip dasar yang harus dipatuhi oleh semua pihak, yaitu:

1) Prinsip pengolahan data yang sah;
2) Prinsip tujuan khusus dan pembatasan;
3) Prinsip kualitas daata;
4) Prinsip pengolahan yang jujur; dan
5) Prinsip akuntabilitas.[32]

Singkatnya, guna menyarikan pemahaman terhadap kelima prinsip kunci ala kawasan ini, tabel berikut ini akan membandingkan prinsip-prinsip yang dimaksud beserta pengaturannya dalam instrumen hukum regional terkait.[33]

Tabel 1: **Prinsip-Prinsip Perlindungan Data Pribadi Uni Eropa**

PRINSIP KUNCI	DASAR HUKUM
1. Prinsip pengolahan data yang sah	- Konvensi 108 (Pasal 5(a)-(b)) - *DP Directive* (Pasal 6(1)(a)-(b))
Sesuai dengan hukum	- *Rotaru v. Romania*, ECtHR (2000) - *Taylor-Saburi v. United Kingdom*, ECtHR (2002)
Mencapai tujuan yang sah	- *Peck v. United Kingdom*, ECtHR (2003)
Dibutuhkan dalam masyarakat yang	- *Khelili v. Switzerland*, ECtHR (2011)

[30] O.J. L. 24, 30 Januari 1998, hal.1-8.
[31] O.J. L. 201, 31 Juli 2002, hal.37–47.
[32] Berbeda halnya dengan *DP Directive*, Konvensi 108 tidak memuat ketentuan terkait dengan prinsip akuntabilitas ini.
[33] Lihat pula CoE dan ECtHR, *Handbook on European Data Protection Law*, (Luxembourg: European Union, 2014) hal.61-62.

demokratis	- *Leander v. Sweden*, ECtHR (1987)
2. Prinsip tujuan khusus dan pembatasan	- Konvensi 108 (Pasal 5(b)) - *DP Directive* (Pasal 6(1)(b))
3. Prinsip kualitas data	
Relevansi data	- Konvensi 108 (Pasal 5(c)) - *DP Directive* (Pasal 6(1)(c))
Ketepatan data	- Konvensi 108 (Pasal 5(d)) - *DP Directive* (Pasal 6(1)(d))
Retensi data yang terbatas	- Konvensi 108 (Pasal 5(e)) - *DP Directive* (Pasal 6(1)(e))
Pengecualian untuk penelitian ilmiah dan statistik	- Konvensi 108 (Pasal 9(3)) - *DP Directive* (Pasal 6(1)(e))
4. Prinsip pengolahan yang jujur	- Konvensi 108 (Pasal 5(a)) - *DP Directive* (Pasal 6(1)(a)) - *Haralambie v. Romania*, ECtHR (2009) - *K.H. and Others v. Slovakia*, ECtHR (2009)
5. Prinsip akuntabilitas	- *DP Directive* (Pasal 6(2))

OECD, sebagai forum untuk negara-negara yang berkomitmen untuk pembangunan demokrasi dan ekonomi pasar, menyediakan pengaturan bagi negara-negara untuk membandingkan praktik-praktik kebijakan, mencari jawaban atas permasalahan bersama, mengidentifikasi praktik-praktik terbaik serta mengoordinasikan segala kebijakan-kebijakan internasional dan dalam negeri. Salah satu buah dari peran OECD dalam memberikan jaminan perlindungan data pribadi adalah dengan membuat *OECD Guidelines* yang berlandaskan pada delapan prinsip utama berikut ini:[34]

1) Prinsip pembatasan pengumpulan data pribadi;
2) Prinsip kualitas data pribadi;
3) Prinsip tujuan khusus penggunaan data pribadi;
4) Prinsip limitasi penggunaan data pribadi;
5) Prinsip perlindungan keamanan;
6) Prinsip keterbukaan;
7) Prinsip partisipasi individu; dan
8) Prinsip akuntabilitas.

Arus informasi sangatlah vital untuk melakukan bisnis dalam era globalisasi ekonomi. Oleh karena itu, maka pada tahun 2004 APEC membuat terobosan dengan merumuskan Kerangka Kerja Privasi APEC atau yang dikenal dengan sebutan*APEC Privacy Framework*.[35] Pendirian kerangka kerja ini didasari pada pentingnya pembangunan perlindungan privasi atas data pribadi yang tepat, utamanya terhadap dampak negatif yang mungkin timbul dari intrusi tanpa izin dan dari penyalahgunaan data pribadi, serta menunjukkan komitmen APEC untuk

[34] *OECD Guidelines*, *Op.Cit.*, para.7-14.
[35] *APEC Privacy Framework*, (2004).

mengakui kebebasan arus informasi sebagai hal yang esensial, baik bagi negara maju dan berkembang, untuk mengembangkan pertumbuhan ekonomi dan sosial. Selain itu, melalui instrumen ini diharapkan dapat memajukan mekanisme internasional yang bertujuan untuk mempromosikan dan menegakkan data privasi dan untuk menjaga kontinuitas arus informasi di antara anggota APEC dan dengan mitra bisnis mereka.[36] Sedikit berbeda dengan instrumen yang dimiliki oleh OECD, *APEC Privacy Framework* memuat sembilan prinsip dasar, yakni:[37]

1) Prinsip pencegahan bahaya;
2) Prinsip pemberitahuan;
3) Prinsip limitasi penggunaan data pribadi;
4) Prinsip penggunaan data pribadi;
5) Prinsip pilihan;
6) Prinsip integritas data pribadi;
7) Prinsip perlindungan keamanan
8) Prinsip akses dan koreksi; dan
9) Prinsip akuntabilitas.

Pada perkembangannya, keberadaan sembilan prinsip ini tidak terlepas dari sejumlah kritik. Greenleaf mencatat setidaknya lima kelemahan dari prinsip-prinsip tersebut di atas. Pembentukan prinsip-prinsip APEC hanya sepenuhnya merujuk kepada prinsip yang termaktub dalam *OECD Guidelines* dengan sedikit perubahan dan mengurangi salah satu prinsip yang termuat dalam instrumen OECD, sehingga hal ini akan memperlemah Pedoman OECD *per se*. Selain itu, instrumen yang dibuat oleh APEC juga masih mengabaikan standar yang berlaku di Eropa, yang dipandang sebagai kawasan yang sukses dalam memberikan jaminan perlindungan data pribadi. Tidak hanya itu, pembentukan *APEC Privacy Framework* juga dinilai gagal dalam mempertimbangkan praktik hukum privasi yang ada di sejumlah negara di Asia-Pasifik, seperti Korea Selatan, Kanada, Hong Kong, Selandia Baru, Taiwan, Australia dan Jepang.[38]

D.2.Praktik perlindungan data pribadi di beberapa negara

Lebih dari 101 negara di dunia, dengan mayoritas negara-negara Eropa, saat ini telah memiliki instrumen hukum yang secara khusus menjamin perlindungan data pribadi.[39] Lebih jauh, untuk melihat beragam praktik pengaturan perlindungan data pribadi di berbagai negara, berikut ini akan diuraikan secara singkat praktik-praktik yang diterapkan pada 10 negara terpilih, yakni:(1) Afrika Selatan, (2) Amerika Serikat, (3) Filipina, (4) Inggris, (5) Jepang, (6) Jerman, (7) Malaysia, (8) Prancis, (9) Swedia dan (10) Republik Rakyat Tiongkok (RRT) yang dapat dijadikan rujukan pembanding dalam membahas perlindungan data pribadi di Indonesia yang akan diuraikan pada bagian berikutnya. Pemilihan terhadap kesepuluh negara ini hanyalah sebatas kepada keterwakilan semua kawasan di dunia, sekaligus relevansi dari praktik di negara tersebut bagi Indonesia.

---

[36] *Id.*, para.8.
[37] *Id.*, para.14-26.
[38] Graham Greenleaf, "Five Years of the APEC Privacy Framework: Failure or Promise?", 25 *Computer L. & Security Rep.* 28, (2009) hal.30-33.
[39] Greenleaf 'Sheherezade', *Op.Cit.*, hal.2.

1) Afrika Selatan

Perlindungan data pribadi di Afrika Selatan diafirmasi oleh Mahkamah Konstitusi Afrika Selatan sebagai bagian dari hak konstitusional atas privasi setiap individu,[40] serta tercermin pada sejumlah bagian undang-undang lainnya.[41] Hingga tulisan ini diterbitkan, Afrika Selatan masih belum memiliki undang-undang yang secara khusus mengatur tentang perlindungan data pribadi. Kendati pada tahun 2013 ditandatangani *Protection of Personal Information Act*(POPI)[42] sebagai upaya menanggapi rekomendasi Komisi Hukum Afrika Selatan (*South African Law Commission*) yang menilai bahwa perlindungan privasi dan data pribadi perlu diatur dalam sebuah kebijakan khusus. Namun, pada bulan April 2014 Presiden Zuma mengumumkan bahwa hanya beberapa bagian dalam PPIA saja yang akan berlaku.[43]

Bagian yang berlaku tersebut adalah sebatas kepada pendirian *Information Regulator* yang bersifat independen dan tidak memihak,[44] serupa dengan *Information Commissioner* yang ada di Inggris.[45] Badan ini memiliki kewenangan untuk:[46] (i) memberikan pengajaran kepada publik, (ii) mengawasi penegakan perlindungan data pribadi berdasarkan ketentuan hukum yang berlaku, (iii) memberikan konsultasi kepada pihak yang berkepentingan, (iv) menerima permohonan gugatan (*complaint*) terkait tuduhan pelanggaran terhadap perlindungan data pribadi, (v) melakukan riset, (vi) membuat ketentuan pelaksananya sendiri atau membantu institusi lain dalam menyusun ketentuan pelaksana institusi tersebut, (vii) melakukan kerja sama lintas batas dalam menegakkan hukum privasi, serta (viii) melaksanakan kewajiban lainnya sebagaimana diatur dalam POPI dan *Promotion of Access to Information Act 2000* (PAIA).[47] Sehubungan dengan pelaksanaan terhadap kewajibannya tersebut, *Information Regulator* bertanggung jawab langsung kepada *National Assembly*, parlemen Afrika Selatan.[48] Sebagai tambahan, sampai tulisan ini diterbitkan badan ini masih belum eksis dan masih dalam proses seleksi anggota *Information Regulator*.[49]

2) Amerika Serikat

Amerika Serikat memiliki sejarah yang panjang dalam memberikan jaminan perlindungan privasi melalui inisiatif-inisiatif pada sejumlah kebijakan yang mereka terapkan, seperti *Privacy Act 1974*[50] yang diterbitkan oleh Kongres Amerika Serikat. Secara khusus tidak terdapat hukum

---

[40] J. Burchell, "The Legal Protection of Privacy in South Africa: A Transplantable Hybrid", 13 *J. Comp. L.* 1 (2009) hal.14.

[41] Sebagai contoh lihat Afrika Selatan, *National Credit Act*, No. 34/2005; Afrika Selatan, *Regulation of Interception of Communications and Provision of Communication-Related Information Act*, No. 70/2002.

[42] Afrika Selatan, *Protection of Personal Information Act*, No.4/2013, (26 November 2013) <http://www.justice.gov.za/legislation/acts/2013-004.pdf> [POPI].

[43] Afrika Selatan, *Proclamation by the President of the Republic of South Africa*, No. R. 25 2014, (17 April 2014) <http://www.gov.za/sites/www.gov.za/files/37544_rg10173_pro25.pdf>.

[44] POPI, *Op.Cit.*, Bagian 39 huruf (b).

[45] Michalsons, "Information Regulator in South Africa", (20 November 2015) <http://www.michalsons.co.za/blog/information-regulator-in-south-africa/13893>.

[46] POPI, *Op.Cit.*, Bagian 40 ayat (1).

[47] Afrika Selatan, *Promotion of Access to Information Act*, No.2/2000, (2 Februari 2000) <http://www.dfa.gov.za/department/accessinfo_act.pdf>.

[48] POPI, *Op.Cit.*, Bagian 39 huruf (d).

[49] "Speech by the Deputy Minister of Justice and Constitutional Development, the Hon JH Jeffery, MP, during the Debate on Vote 21: Justice and Constitutional Development, National Assembly", (19 Mei 2015) <http://www.justice.gov.za/m_speeches/2015/20150519_BudgetVoteDM.html>.

[50] Amerika Serikat, *Privacy Act*, 5 U.S.C. 552a, (31 Desember 1974) <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf> [*Privacy Act 1974*].

nasional yang secara komprehensif memuat pengaturan tentang pengelolaan dan penggunaan data pribadi, tetapi konsep ini telah tercampur aduk bersama dengan sejumlah undang-undang federal dan regulasi lain yang tak jarang bertumpang tindih, berkesesuaian atau bahkan bertentang satu sama lain.[51] Hal ini berimplikasi pada tidak adanya keseragaman definisi data pribadi dalam sistem hukum di Amerika Serikat itu sendiri.[52]

Tidak hanya bertumpu pada instrumen hukum yang mengikat saja, perlindungan data pribadi di Amerika Serikat juga sering kali merujuk pada pedoman-pedoman yang diterbitkan oleh agen pemerintah dan kelompok industri, yang tidak mengikat secara hukum, namun telah dipertimbangkan sebagai praktik terbaik dalam melindungi data pribadi.

Sehubungan dengan *Privacy Act 1974*, instrumen ini nyatanya hanya memuat ketentuan pembatasan pengumpulan dan penggunaan informasi pribadi sebatas kepada agen-agen pemerintah federal. Dengan kata lain, undang-undang ini tidak berlaku bagi pengumpulan dan penggunaan data pribadi yang dilakukan oleh pihak swasta.[53]

Pada prinsipnya, undang-undang ini melarang setiap agen pemerintah untuk membuka setiap catatan yang berhubungan dengan data pribadi seseorang tanpa persetujuan pemegang data yang bersangkutan.[54] Pengecualian terhadap pembukaan data pribadi tersebut adalah sebatas kepada dua belas alasan-alasan di bawah ini, yaitu:[55]

1) Untuk agen pemerintah federal yang mengelola pencatatan terhadap data yang perlu untuk dicatatkan tersebut;
2) Pembukaan data berdasarkan ketentuan dalam undang-undang ini;
3) Untuk kebutuhan rutin setiap agen-agen federal;
4) Untuk kebutuhan statistik oleh Badan Sensus (*Census Bureau*);
5) Untuk pihak yang telah memberikan pemberitahuan yang cukup terlebih dahulu kepada agen federal bahwa catatan tersebut akan digunakan untuk keperluan penelitian atau pelaporan;
6) Untuk kebutuhan *National Archives and Records Administration* dalam pengarsipan terhadap catatan yang memiliki nilai sejarah;
7) Untuk kebutuhan agen-agen di bawah kontrol Amerika Serikat dalam penegakan hukum perdata atau pidana;
8) Pembukaan data karena alasan mendesak (*compelling circumstances*) yang mempengaruhi kesehatan atau keamanan seseorang;
9) Untuk kebutuhan Kongres atau [sub]-komite di bawah mandat Kongres;
10) Untuk kebutuhan bagi Badan Pengawas Keuangan (*Comptroller General*) dalam melaksanakan kewajiban *General Accounting Office*;
11) Pembukaan data atas dasar perintah pengadilan; dan
12) Untuk agen-agen pelaporan konsumen (*consumer reporting agencies*/CRAs) sesuai dengan ketentuan 31 U.S.C. 3711(e).

---

[51] Paul M. Schwartz dan Daniel J. Solove, "Reconciling Personal Information in the United States and European Union", 102 *Calif. L. Rev.* 877 (2014) hal.887-891 [Schwartz dan Solove (2014)].

[52] *Id*.

[53] Thomas J. Smedinghoff (ed.), *Online Law: The SPA's Legal Guide to Doing Business on the Internet*, (Reading: Addison-Wesley Developers Press, 1996) hal.273.

[54] Edmon Makarim, *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*, (Jakarta: PT. RajaGrafindo Persada, 2005) hal.174 [Edmon Makarim].

[55] *Privacy Act 1974*, *Op.Cit.*, Sub-bagian (b).

Guna menjamin bahwa ketentuan ini dapat terimplementasikan dengan baik, maka *Privacy Act 1974* memandatkan *Office of Management and Budget* (OMB) untuk (i) membuat panduan dan regulasi yang dapat digunakan oleh setiap agen federal untuk mengimplementasikan undang-undang ini, serta (ii) melakukan pemantuan terhadap penegakan ketentuan ini.[56]

Tidak hanya itu, upaya pemantauan yang ketat terkait perlindungan data pribadi dari instansi pemerintahan juga dapat ditempuh melalui suatu badan bernama *Data Integrity Boards* yang wajib dibentuk oleh masing-masing agen pemerintah federal.[57] Agen privasi ini berwenang untuk memantau sekaligus mengkoordinasikan terhadap semua komponen terkait pelaksanaan kewajiban agen federal yang bersangkutan terhadap ketentuan dalam undang-undang ini.[58]

Instrumen lain yang dapat dijadikan rujukan dalam menjamin penikmatan terhadap hak atas privasi, khususnya dalam hal perlindungan data pribadi, atas segala macam bentuk gangguan yang dilakukan oleh non-pemerintah (baik pihak swasta dan perorangan) dapat terlihat dalam *Video Privacy Protection Act* (VPPA), *Children's Online Privacy Protection Act* (COPPA), *Telephone Consumer Protection Act* (TCPA), *Controlling the Assault of Non-Solicited Pornography and Marketing Act* (*CAN-SPAM*), *Financial Services Modernization Act* (*Gramm-Leach-Bliley Act*/GLB), *Fair Credit Reporting Act* (FCRA), *Health Insurance Portability and Accountability Act* (HIPAA) dan *Electronic Communication Privacy Act* (ECPA).

Selain itu, ada pula beberapa instrumen hukum lain yang berlaku secara khusus bagi setiap negara bagian, sebagai contoh, *California Online Privacy Protection Act* (Cal. COPPA), *California Financial Information Privacy Act* (CFPIA), *Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth* dan *New York General Business Law*.

3) Filipina

Pada 15 Agustus 2012, Presiden Benigno Aquino juga telah menandatangani Undang-Undang No. 10173 (*Republic Act No. 10173*) Tahun 2012 tentang Data Pribadi (*Data Privacy Act 2012*),[59] yang disetujui oleh Kongres Filipina. Meski sebelumnya peraturan perundang-undangan Filipina telah mengatur perlindungan terhadap keamanan data pribadi seseorang, namun undang-undang inilah yang pertama kali memperkenalkan rezim kerahasiaan data di Filipina.

Menurut undang-undang ini, segala bentuk pemindahtanganan data akan tunduk pada prinsip-prinsip akuntabilitas. Prinsip ini menegaskan bahwa setiap pihak yang menyimpan atau memiliki otoritas atas suatu informasi pribadi bertanggungjawab atas informasi pribadi tersebut di bawah kontrolnya, termasuk juga informasi yang telah dialihkan kepada pihak ketiga untuk dilakukan pengolahan, baik yang sifatnya domestik maupun internasional.[60]

---

[56] *Id.*, Sub-bagian (v).

[57] Untuk rincian badan pengawas yang dimiliki oleh *Data Integrity Boards* dalam setiap agen-agen Federal di Amerika Serikat dapat dilihat pada <https://cio.gov/about/groups/privacy-cop/privacy/>.

[58] *Privacy Act 1974, Op.Cit.*, Sub-bagian (u) ayat (1).

[59] Filipina, *Data Privacy Act*, No.10173, (15 Agustus 2012) <http://www.gov.ph/2012/08/15/republic-act-no-10173/>.

[60] *Id.*, Bab VI, Bagian 21.

Undang-undang ini berlaku untuk semua jenis informasi dan semua entitas, baik individu, publik maupun swasta, yang terlibat dalam pengololaan informasi pribadi. Tunduk dalam ruang lingkup pengaturan ini juga termasuk penyedia *server* yang berada di luar Filipina, atau yang sekadar memiliki kantor perwakilan di Filipina.[61] Termasuk informasi yang dimiliki oleh jurnalis serta narasumbernya juga dilindungi menurut undang-undang ini.[62]

Ketentuan undang-undang ini juga secara detail mengatur hak-hak dari pemilik informasi pribadi (subjek data), seperti hak untuk diberitahukan apabila sedang dilakukan pengolahan terhadap informasi pribadinya, dimintakan persetujuan terlebih dahulu sebelum informasi pribadinya dimasukan ke dalam sistem, mengenai sejumlah hal yang meliputi: (a) informasi pribadi yang akan dimasukkan ke dalam sistem; (b) tujuan dari proses tersebut; (c) lingkup dan metode pengolahan informasi pribadi; (d) penerima atau tingkat penerima dari informasi tersebut; (e) metode yang digunakan untuk akses otomatis, jika diperbolehkan oleh pemilik data, dan sejauhmana akses tersebut dibolehkan; (f) identitas dan rincian kontak pengelola informasi pribadi atau yang mewakili; (g) lamanya periode penyimpanan informasi pribadi; dan (h) hak-hak pemilik data untuk mengakses, mengoreksi, serta hak komplain ke Komisi.[63]

Komisi yang dimaksud menurut undang-undang ini adalah Komisi Privasi Nasional (*National Privacy Commission*) di dalam Departemen Perhubungan dan Komunikasi (*Department of Information and Communications Technology/DICT*), yang dibentuk berdasarkan Bab II Bagian 7 *Data Privacy Act 2012*. Komisi ini sendiri berfungsi untuk mengelola dan melaksanakan ketentuan undang-undang, serta memantau dan memastikan kepatuhan negara terhadap standar internasional yang ditetapkan dalam perlindungan data. Lebih jauh, lembaga ini berfungsi seperti layaknya lembaga kuasi-yudisial lainnya yang bertugas menerima pengaduan, melakukan investigasi atas suatu pengaduan, dan memfasilitasi proses penyelesaian sengketa alternatif untuk menetapkan besaran ganti kerugian yang layak jika terjadi suatu pelanggaran. Komisi juga berwenang untuk mengeluarkan larangan sementara atau permanen terhadap pengolahan informasi pribadi, jika pengolahan tersebut diduga akan merugikan keamanan nasional dan kepentingan umum. Lembaga ini bertanggung jawab pula untuk mengkoordinasikan seluruh pemangku kepentingan dalam penyiapan rencana kebijakan perlindungan data di dalam negeri, termasuk memberikan usulan amandemen undang-undang terkait data pribadi. Persyaratan privasi yang digunakan oleh suatu badan publik atau swasta dalam pengolahan informasi pribadi seseorang juga diuji oleh Komisi ini.[64]

Ketentuan pidana juga diatur di dalam undang-undang ini, sebagaimana terumuskan di dalam Bab VIII, yang menyebutkan mengenai rincian denda atas pelanggaran undang-undang, juga ancaman hukuman penjara. Pelanggaran terhadap *Data Privacy Act 2012* termasuk pengolahan yang tidak sah dari suatu informasi pribadi, akses yang tidak sah, penghancuran informasi pribadi secara tidak tepat, pelanggaran keamanan terhadap informasi sensitif dan peng-ungkapan informasi secara tidak sah. Pelanggaran terhadap ketentuan undang-undang ini diancam pidana denda antara lima ratus ribu (Php 500.000,00) sampai dengan lima juta peso Filipina (Php 5.000.000,00), juga ancaman pidana penjara sedikitnya satu tahun enam bulan atau selama-lamanya tujuh tahun. Jika pelanggaran dilakukan oleh korporasi maka tanggung

[61] *Id.*, Bagian 4.
[62] *Id.*, Bagian 5.
[63] *Id.*, Bab IV, Bagian 16.
[64] Rincian selengkapnya mengenai tugas dan fungsi dari Komisi Privasi Nasional Filipina dapat dilihat dalam Bab II *Data Privacy Act 2012*.

jawab pidana ada pada individu yang memiliki tanggung jawab dalam pengolahan data atau pihak yang turut serta mensponsori terjadinya pelanggaran. Selain itu, terhadap korporasi pengadilan juga dapat mencabut ijin serta hak-hak yang dimiliki korporasi tersebut menurut undang-undang ini. Apabila pelakunya adalah warga negara asing, maka dia harus dilakukan deportasi setelah selesai menjalani hukuman.[65]

4) Inggris

Di Inggris, pengaturan terkait perlindungan data pribadi telah dijamin dalam *Data Protection Act 1998*[66] (DPA) yang menggantikan *DPA 1994*. Perubahan mendasar antara DPA 1998 dengan DPA 1994 ini setidaknya dalam ketentuan yang baru memuat pengaturan yang juga berlaku bagi data yang diproses secara manual. Selain itu, DPA 1998 juga memuat kategorisasi terhadap data sensitif, serta memberikan larangan pengiriman data ke negara lain yang tidak memiliki mekanisme perlindungan data yang cukup.[67]

Menurut DPA 1998, data sensitif didefinisikan sebagai data pribadi seseorang yang mengandung informasi terkait (a) identitas ras atau etnis; (b) pandang politik; (c) keyakinan agama atau kepercayaan lain; (d) keanggotaan dalam suatu serikat kerja; (e) kondisi kesehatan fisik atau mental; (f) kehidupan seksual; atau (g) catatan perbuatan kriminal.[68]

Dalam menjamin upaya perlindungan data di Inggris, DPA 1998 juga memberikan delapan prinsip dasar yang harus diperhatikan oleh pengontrol data (*data controller*).[69] Kedelapan prinsip-prinsip tersebut adalah:[70]

1) Data pribadi harus diperoleh secara jujur dan sah, dengan tetap mempertimbangkan ketentuan dalam Skedul 2 dan 3;
2) Data pribadi harus dimiliki hanya untuk satu tujuan atau lebih yang spesifik dan sah, dan tidak boleh diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan-tujuan tersebut;
3) Data pribadi harus layak, relevan dan tidak terlalu luas dalam hubungannya dengan tujuan atau tujuan-tujuan pengolahannya;
4) Data pribadi harus akurat dan jika perlu selalu *up-to-date*;
5) Data pribadi harus diproses sesuai dengan tujuannya dan tidak boleh dikuasai lebih lama dari waktu yang diperlukan untuk kepentingan tujuan atau tujuan-tujuan tersebut;
6) Data pribadi harus diproses sesuai dengan hak-hak dari subjek data sebagaimana yang diatur dalam undang-undang ini;
7) Tindakan-tindakan pengamanan yang memadai harus diambil untuk menghadapi kegiatan pemrosesan data pribadi yang tidak sah serta atas kerugian yang tidak terduga atau kerusakan dari data pribadi; dan

---

[65] Selengkapnya lihat Bab VIII *Data Privacy Act 2012*.
[66] Inggris, *Data Protection Act*, (16 Juli 1998) <http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf> [DPA 1998].
[67] Edmon Makarim, *Op.Cit.*, hal.171.
[68] DPA 1998, *Op.Cit.*, Bagian 2.
[69] *Id.*, Bagian 4.
[70] *Id.*, Skedul 1.

8) Data pribadi tidak boleh dikirim ke negara atau wilayah lain di luar Wilayah Ekonomi Eropa, kecuali jika negara atau wilayah tersebut menjamin dengan suatu tingkat perlindungan terhadap hak-hak dan kebebasan-kebebasan subjek data sehubungan dengan pemrosesan data.

DPA 1998 turut pula mengatur hak-hak subjek data (pemilik data pribadi) dalam ketentuan pada Bab II. Hak-hak dari pemilik data pribadi tersebut mencakup: (a) hak atas akses terhadap data pribadi;[71] (b) hak untuk mencegah pemrosesan yang dapat menimbulkan kerusakan atau keadaan membahayakan;[72] (c) hak untuk mencegah pemrosesan untuk tujuan pemasaran langsung (*direct marketing*);[73] (d) hak berkaitan dengan pengambilan keputusan oleh *data controller* secara langsung tanpa mempertimbangkan kepentingan subjek data;[74] (e) hak terkaitpengecualian terhadap data manual;[75] (f) kompensasi;[76] (g) hak untuk rektifikasi, pemblokiran, penghapusan dan penghancuran data;[77] dan (h) hak untuk memohon kepada *Information Commissioner's Office* (ICO)[78] untuk membuat penyelesaian terhadap tindakan-tindakan yang melanggar ketentuan-ketentuan dalam undang-undang ini.[79]

Khusus untuk konteks mekanisme penegakan, DPA 1998 memberikan dua alternatif solusi, yakni, *pertama*, dengan mendirikan *Data Protection Commissioner* yang kemudian diubah namanya menjadi ICO. *Kedua*, melalui institusi yudisial bernama *Information Tribunal*.[80] Sehubungan dengan hal ini, Bagian 51 ayat (1) DPA 1998 telah menegaskan fungsi utama ICO sebagai badan yang berwenang untuk melakukan pemantauan terhadap pemenuhan kewajiban-kewajiban *data controller* sebagaimana diatur dalam undang-undang ini. Jika ditemukan ketidaksesuaian dengan ketentuan DPA 1998, ICO berkewajiban untuk menerbitkan suatu surat peringatan baik berupa *enforcement notice*,[81] *assessment notice*,[82] *information notice*[83] atau *special information notice*.[84] Jika pihak yang menerima surat peringatan ini telah diterbitkan, maka ia dapat mengajukan banding kepada *Information Tribunal*.[85] Namun, pada perkembangannya, khususnya sejak tahun 2010, ICO dapat menjatuhkan sanksi kepada pelanggar ketentuan dalam undang-undang ini.[86]

5) Jepang

Pengaturan terhadap perlindungan data pribadi di Jepang sejatinya dapat dilihat pada instrumen hukum yang dimilikinya. Sejauh ini, Jepang telah memiliki *Act on the Protection of*

---

[71] *Id.*, Bagian 7-9A.
[72] *Id.*, Bagian 10.
[73] *Id.*, Bagian 11.
[74] *Id.*, Bagian 12.
[75] *Id.*, Bagian 12A.
[76] *Id.*, Bagian 13.
[77] *Id.*, Bagian 14.
[78] Informasi lebih lanjut mengenai institusi ini dapat diakses pada <https://ico.org.uk>.
[79] DPA 1998, *Op.Cit.*, Bagian 42.
[80] *Id.*, Bagian 6.
[81] *Id.*, Bagian 40.
[82] *Id.*, Bagian 41A.
[83] *Id.*, Bagian 43.
[84] *Id.*, Bagian 44.
[85] *Id.*, Bagian 48.
[86] Lihat BBC, *First Data Protection Act fines issued by commissioner*, (24 November 2010) <http://www.bbc.com/news/uk-11821203>.

Personal Information (APPI)[87] yang bertujuan untuk melindungi hak-hak dan kepentingan-kepentingan individu,[88] kaitannya dengan penggunaan data pribadi milik individu yang bersangkutan tersebut oleh *data controller*.[89]

Uniknya, *data controller* yang dimaksud dalam undang-undang ini hanyalah sebatas kepada pelaku bisnis yang menggunakan data pribadi sebagai kegiatan usahanya dan mengecualikan (i) organ negara, (ii) pemerintah daerah, (iii) badan administratif independen (nasional dan daerah),[90] serta (iv) pihak yang tidak menggunakan data pribadi milik lebih dari 5.000 individu selama enam bulan terakhir.[91] Selain itu, pengecualian terhadap keberlakuan undang-undang ini juga diterapkan bagi pengunaan data pribadi untuk (i) kepentingan jurnalistik oleh institusi penyiaran, penerbit surat kabar, kantor berita dan anggota pers lainnya; (ii) kegiatan kesusastraan; (iii) studi ilmiah oleh universitas dan institusi akademis lainnya; (iv) organisasi keagamaan yang melakukan kegiatan keagamaan; dan (v) kegiatan politik yang dilakukan oleh organisasi politik.[92]

Jika dibandingkan dengan pengaturan di Eropa, materi muatan dalam APPI jelas masih belum sempurna. Meskipun Pasal 2 ayat (3) APPI mewajibkan *data controller* untuk mendapatkan persetujuan dan memberikan notifikasi kepada subjek data, serta pengumuman kepada publik terkait penggunaan data pribadi. Akan tetapi, APPI tidak mewajibkan pengguna data tersebut untuk memberikan notifikasi atau mendaftarkan data yang dimaksud kepada instansi pemerintah Jepang sebelum pengolahhan data tersebut dilakukan. Hal ini diperparah dengan tidak adanya keseragaman dalam metode untuk memperoleh persetujuan dari subjek data.[93]

Tidak hanya itu, kelemahan lain terkait dengan instrumen APPI ini adalah tidak adanya pasal yang secara spesifik memberikan mandat bagi badan tertentu yang secara khusus memiliki kewenangan untuk melakukan supervisi terhadap penegakan ketentuan dalam undang-undang tersebut. Sehingga, praktis perlindungan data pribadi di Jepang, hingga saat ini, masih bertumpu pada mekanisme pengawasan yang disediakan oleh masing-masing kementerian, yang cenderung muatannya tumpang-tindih dan tak jarang malah bertentangan satu sama lain. Sampai bulan Juli 2010 saja, setidaknya terdapat sekitar 40 Panduan (*Guidelines*) yang diterbitkan oleh semua kementerian dan organ pemerintahan yang terkait dengan praktik pemindahtanganan data pribadi.[94]

Oleh karena itu, pada 9 September 2015, Parlemen Jepang (*Kokkai*) mengesahkan Amandemen APPI[95] yang secara materiil memberikan perubahan mendasar bagi perlindungan data pribadi

---

[87] Jepang, *Act on the Protection of Personal Information*, No. 57, (30 Mei 2003) <http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf> [APPI].

[88] *Id.*, Pasal 1.

[89] *Id.*, Pasal 2-3.

[90] *Id.*, Pasal 18(1).

[91] Jepang, *Cabinet Order for the enforcement of the Act on the Protection of Personal Information*, No. 507, (10 Desember 2003) <http://www.worldlii.org/int/other/PrivLRes/2003/2.html> Pasal 2.

[92] APPI, *Op.Cit.*, Pasal 50(1).

[93] Bandingkan Jepang, *Ministry of Economy, Trade and Industry (METI) Guidelines*, No. 2, (9 Oktober 2009) Bagian 2(1)(10); Jepang, *Ministry of Labour, Health and Welfare (MLHW) Guidelines for Medical and Nursing Enterprises*, (24 Desember 2004) Bagian III(1)(2)(4); Jepang, *Financial Service Agency (FSA) Privacy Guidelines*, (20 November 2009) Pasal 13(1).

[94] Sayuri Umeda, "Online Privacy Law: Japan", Library of Congress, (Juni 2002) <https://www.loc.gov/law/help/online-privacy-law/japan.php#_ftn10>.

[95] Jepang, *Amendment Act on the Protection of Personal Information*, (9 September 2015) <http://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf> [Amandemen APPI].

di Jepang. Ketentuan terbaru ini baru akan resmi berlaku terhitung sejak 9 September 2017 mendatang.

Pengaturan yang mengalami modifikasi dalam Amandemen APPI ini setidaknya mencakup enam hal.[96] Pertama, Amandemen APPI membedakan antara data pribadi dan data sensitif.[97] Kedua, adanya ketentuan terkait dengan metode perlakuan terhadap data anonim (*de-identified information*).[98] Ketiga, pengetatan syarat-syarat untuk memindahtangankan data tanpa persetujuan subjek data (*opt-out policy*), termasuk kewajiban untuk mempublikasikan *opt-out policy* tersebut.[99] Keempat, ketentuan untuk menjamin kemampuan subjek data untuk melacak kemana data pribadinya dipindahtangankan.[100] Kelima, pendirian *Personal Information Protection Commission* (PIPC)[101] sebagai badan sentral yang berwenang untuk melakukan supervisi terhadap perlindungan data pribadi di Jepang, termasuk berkewajiban untuk melakukan harmonisasi ketentuan-ketentuan yang telah dimiliki selama ini terkait mekanisme penegakan data pribadi.[102] Keenam, berlakunya APPI untuk lintas batas negara,[103] sekaligus diaturnya ketentuan terkait dengan pemindahtanganan data pribadi ke luar wilayah Jepang.[104]

6) Jerman

Perlindungan data pribadi di Jerman diawali dengan pengesahan *Hessisches Datenschutz-gesetz* (*Hesse Data Protection Act*) 1970 yang berlaku khusus untuk negara bagian federasi Hesse. Pengesahan ini dilatarbelakangi oleh kekhawatiran publik terhadap rencana pemerintah setempat untuk melakukan penyimpanan data penduduk Hesse melalui media komputer.[105] Hal ini yang kemudian mendorong lahirnya *Federal Data Protection Act*(FDPA)[106] yang berlaku di seluruh wilayah Jerman.

Meskipun dipandang sebagai undang-undang pelopor yang memberikan jaminan perlindungan terhadap data pribadi,[107] nyatanya preposisi ini masih sukar untuk diterima, mengingat undang-undang tersebut tidak secara eksplisit memuat rujukan perihal hak atas privasi.[108] Pada perkembangannya, barulah pada tahun 1990 ketika Mahkamah Konstitusi Jerman mengakui perlindungan konstitusional terhadap data pribadi;[109] maka ketentuan FDPA

---

[96] John C. Roebuck, et al, "Japan: Amendment of the Personal Information Protection Act", Jones Day, (4 November 2015) <http://www.mondaq.com/x/440786/Data+Protection+Privacy/Amendment+of+the+Personal+Information>.
[97] Amandemen APPI, *Op.Cit.*, Pasal 2(1),(3).
[98] *Id.*, Pasal 36-39.
[99] *Id.*, Pasal 23(1).
[100] *Id.*, Pasal 25-26.
[101] Informasi lebih lanjut mengenai Komisi ini dapat diakses pada <http://www.ppc.go.jp/en/>.
[102] Amandemen APPI, *Op.Cit.*, Bab V.
[103] *Id.*, Pasal 75.
[104] *Id.*, Pasal 24.
[105] F.W. Hondius dan F.W. Hondius, *Emerging Data Protection in Europe*, (Amsterdam: North-Holland Pub. Co., 1975) hal.35.
[106] Jerman, *Federal Data Protection Act (Bundesdatenschutzgesetz)*, (27 Januari 1977) <http://www.gesetze-im-internet.de/englisch_bdsg/> [FDPA].
[107] J. Lee Riccardi, "The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?", 6 *B.C. Int'l & Comp. L. Rev.* 1 (1983) hal.248.
[108] Viktor Mayer-Schönberg, "Generational development of data protection in Europe", dalam Philip E. Agre dan Marc Rotenberg (eds.), *Technology and Privacy: The New Landscape*, (Cambridge: MIT Press, 1997) hal.224.
[109] *Census Act (Volkszählung)*, BVerfGE 65, 1 (1983).

mengalami perubahan[110] dan secara tegas menempatkan jaminan hak atas privasi atas segala macam bentuk pemindahtanganan data pribadi seseorang.[111]

Secara substantif, ketentuan dalam FDPA hanya berlaku tidak hanya pada agen federal Jerman saja, tetapi juga kepada pihak swasta.[112] Hal ini tercermin dalam Bagian 1 ayat (2) FDPA itu sendiri yang menyatakan bahwa undang-undang ini berlaku bagi pengumpulan, pengolahan dan penggunaan data pribadi oleh (i) badan publik Federasi Jerman,[113] (ii) pejabat publik negara bagian federal[114] dan (iii) badan non-publik lainnya.[115]

Aktualisasi diri dari penegakan undang-undang ini kemudian diserahkan kepada Komisioner Federal untuk Perlindungan Data dan Kebebasan Informasi atau *Federal Commissioner for Data Protection and Freedom of Information* (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit/BfDI*)[116] yang tunduk kepada Kementerian Federal Dalam Negeri.[117]BfDI merupakan badan pengawas independen[118] yang melakukan pemantauan dan memberikan masukan kepada pejabat publik federal, pejabat publik lainnya yang berada di bawah kuasa pemerintah negara federal, serta penyedia jasa layanan telekomunikasi dan pos sebagaimana ditentukan oleh *Telecommunications Act* (*Telekommuni-kationsgesetz/TKG*) dan*Postal Law* (*Postgesetz/PostG*).[119] Kendati tidak memiliki kewenangan untuk menerima gugatan, BfDI tetap dapat menyampaikan temuan-temuannya di lapangan kepada otoritas yang berwenang sebagaimana tertuang dalam Bagian 25 ayat (1) FDPA.

7) Malaysia

Konstitusi Malaysia tidak secara tegas memberikan perlindungan terhadap hak atas privasi warga negaranya. Sementara KUHP Malaysia secara terbatas hanya mengatur bahwa seseorang yang mencampurtangani privasi orang lain dapat dipidana denda atau penjara selama-lamanya lima tahun atau dapat dikenakan kedua-duanya.[120] Kaitannya dengan perlindungan data pribadi warga negara, pada tahun 2010 Parlemen Malaysia telah mengesahkan Undang-Undang No. 709 Tahun 2010 tentang Perlindungan Data Pribadi (*Personal Data Protection Act 2010/PDPA*),[121] dan dinyatakan mulai berlaku terhitung sejak 16 Agustus 2013, dengan masa transisi tiga bulan.[122] Undang-undang ini mengatur dengan detail prinsip-prinsip perlindungan data pribadi, hak-hak pemilik data,[123] tata cara pemindah-tanganan data, serta kewajiban bagi

---

[110] Perubahan terhadap FDPA ini bahkan harus dilalui dengan tiga kali amandemen, yakni Amandemen I (1990), Amandemen II (2001) dan Amandemen III (2009).
[111] FDPA, *Op.Cit.*, Bagian 1(1).
[112] *Id.*, Bagian 1(2).
[113] Pengecualian terhadap ketentuan FDPA ini hanyalah berlaku bagi *Central Register of Foreign Nationals* semata, sesuai dengan Bagian 22 dan 37 FDPA.
[114] FDPA, *Op.Cit.*, Bagian 2(2).
[115] *Id.*, Bagian 2(4).
[116] Informasi lebih lanjut mengenai badan ini dapat diakses pada <http://www.bfdi.bund.de>.
[117] FDPA, *Op.Cit.*, Bagian 22(5).
[118] *Id.*, Bagian 22(4).
[119] *Id.*, Bagian 24 dan 26(3).
[120] Malaysia, *Penal Code (Amendment) Act 2012*, No.574, (31 Juli 2012) <http://www.vertic.org/media/National%20Legislation/Malaysia/MY_Criminal_Code_2013.pdf> Bagian 509.
[121] Malaysia, *Personal Data Protection Act*, No.709, (2 Juni 2010) <http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf> [PDPA 2010].
[122] Graham Greenleaf, "Malaysia: ASEAN's first data privacy Act 2010 in force", 126 *Privacy L. & Bus. Int'l Rep.* 11 (2013) hal.2.
[123] PDPA 2010, *Op.Cit.*, Pasal 30.

pihak-pihak yang melakukan penyimpanan data.Di dalamnya juga diatur mengenai mekanisme komplain bagi seseorang yang data pribadinya dipindahtangankan secara tidak sah.[124]

Melalui undang-undang ini juga dibentuk Komite Penasihat Perlindungan Data Pribadi yang bertugas menerima laporan jika terjadi penyalahgunaan dan pemindahtangananan data pribadi secara melawan hukum,[125] juga sekaligus dibentuk pengadilan banding dalam konteks penyelesaian secara yudisial.[126] Tidak hanya memberikan ruang komplain, undang-undang ini juga memberikan ancaman pidana bagi setiap orang yang melakukan pelanggaran terhadap ketentuan perlindungan data pribadi. Ancaman terberat misalnya ditujukan bagi pihak yang tanpa ijin mengakses data pribadi pihak lain, atau mengumpulkan data pribadi secara melawan hukum, pelakunya dapat dipidana denda sampai dengan lima ratus ribu ringgit Malaysia dan/atau penjara selama-lamanya tiga tahun.[127]

8) Prancis

Pada tahun 1978, Pemerintah Prancis membentuk suatu Undang-Undang Nomor 78-17 bernama *Law on Computers, Files and Freedoms*(UU 78-17),[128] yang memberikan jaminan perlindungan data pribadi dalam media komputer sebagai konsekuensi logis dari lahirnya kebijakan SAFARI (*Système Automatisé pour les Fichiers administratifs et le Répertoire des Individus*)[129] dan GAMIN (*Gestion Automatiséee de la Médicine Infantile*)[130] yang dinilai dapat mengacam hak privasi terhadap data personal masyarakat Prancis.

Seperti halnya di Inggris, UU 78-17 juga memberikan pembatasan terhadap ruang gerak bagi pihak-pihak yang akan memindahtangankan suatu data pribadi, seperti *data controller*. Selain mendapatkan persetujuan dari subjek data,[131] pemindahtanganan data pribadi harus pula mempertimbangkan lima hal pokok di bawah ini:[132]

1) Data pribadi harus diperoleh dan dikelola secara jujur dan sah;
2) Penggunaan data pribadi hanya untuk tujuan yang spesifik, jelas dan sah;
3) Pengambilan dan pengelolaan data pribadi harus layak, relevan dan tidak melebihi tujuan yang ingin dicapai;
4) Data pribadi harus akurat dan jika dibutuhkan selalu *up-to-date*; dan
5) Data pribadi tidak boleh dikuasai lebih lama dari waktu yang diperlukan untuk kepentingan tujuan tersebut.

---

[124] *Id.*, Pasal 31 dan 104.
[125] *Id.*, Bagian VI.
[126] *Id.*, Bagian VII.
[127] *Id.*, Pasal 130.
[128] Prancis, *Law on Computers, Files and Freedoms (Loi relative à L'informatique, aux Fichiers et aux Libertés)*, No.78-17, (6 Januari 1978) <https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf> [UU 78-17].
[129] Henri Delahaie dan Félix Paoletti, *Informatique et Libertés*, (Paris: Editions La Découverte, 1987) hal.20.
[130] Herbert Burkert, "Privacy/Data Protection: A German/European Perspective", pada *Proceedings of 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council, Wood Hole, Massachusets*, (1999) hal.50.
[131] UU 78-17, *Op.Cit.*, Pasal 7.
[132] *Id.*, Pasal 6.

Guna menjamin implementasi undang-undang ini dengan baik, ketentuan dalam Bab III menunjukkan eksistensi suatu badan administratif independen bernama Komisi Nasional Informasi dan Kebebasan atau *National Commission on Informatics and Liberty* (*Commission Nationale Informatique et Libertés/CNIL*).[133] Menurut UU 78-17, CNIL memiliki dua tugas utama, yaitu: (i) untuk memantau implementasi undang-undang ini,[134] dan (ii) memberikan sanksi bagi pelanggarnya.[135]

Selain pembentukan CNIL, upaya penegakan hukum terkait dengan perlindungan data pribadi melalui undang-undang ini ditempuh dengan pemuatan ketentuan pidana bagi setiap pelanggar UU 78-17. Untuk pelanggaran terhadap ketentuan materiil undang-undang ini dapat dikenakan pidana Pasal 226 ayat (16)-(24) KUHP Prancis.[136] Sementara, untuk pelanggaran terkait dengan hal-hal yang menghambat segala kerja CNIL dapat dipenjara sampai satu tahun dan membayar denda sebesar lima belas ribu Euro (€15.000,00).[137]

9) Swedia

Kendati KUHP Swedia memberikan jaminan pengaturan atas segala macam bentuk tindakan defamasi.[138] Perlindungan data pribadi baru secara nyata diatur pada tahun 1973 ketika diterbitkanya*Datalag* (*Data Act*)[139] sebagai upaya merespon konsensus publik pada tahun 1969 dan menindaklanjuti laporan Komisi Parlemen Swedia berjudul "*Data och integritet*" pada tahun 1972.[140] Selain itu, pemberlakuan *Datalag* ini juga dipengaruhi dengan mulai dibangunnya suatu sistem identifikasi kependudukan di tengah berkembangnya era digitalisasi administrasi publik *vis-à-vis* dengan era keterbukaan publik dalam mengakses dokumen pemerintah berlandaskan prinsip akses publik (*offentlighetsprincip*).[141]

Pada perkembangannya, *Data Act* tersebut dicabut dan diganti dengan *Personal Data Act 1998* (PDA 1998).[142] Berbeda dengan *Datalag*, PDA 1998 menekankan bahwa instrumen ini berlaku tidak hanya untuk data pribadi yang secara otomatis diproses, tetapi juga untuk data-data pribadi yang secara manual didaftarkan.[143] Perubahan mendasar dalam sistem hukum di Swedia ini, nyatanya dipengaruhi oleh lahirnya *DP Directive* yang berlaku bagi seluruh negara anggota Uni Eropa, termasuk Swedia.[144]

Dalam melakukan pengolahan data pribadi, DPA 1998 menentukan bahwa pihak *data controller* berkewajiban untuk menjamin data tersebut hanya akan diproses jika (i) hal

---

[133] Informasi lebih lanjut mengenai CNIL dapat diakses pada <https://www.cnil.fr>.
[134] UU 78-17, *Op.Cit.*, Bab VI.
[135] *Id.*, Bab VII.
[136] *Id.*, Pasal 50.
[137] *Id.*, Pasal 51.
[138] Swedia, *Penal Code*, SFS 1962:700, (1962) <http://www.government.se/contentassets/5315d27076c942019828d6c36521696e/swedish-penal-code.pdf> Bab 5.
[139] Swedia, *Data Act (Datalag)*, SFS 1973:289, (11 Mei 1973).
[140] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, (Heidelberg: Springer, 2014) hal.58.
[141] Jonathan Steele, "Data Protection: An Opening Door? The Relationship Between Accessibility and Privacy in Sweden in an EU perspective", 24 *Liverpool L. Rev.* 19 (2002) hal.19.
[142] Swedia, *Personal Data Act*, SFS 1998:204, (29 April 1998).
[143] Ministry of Justice, Sweden (Regeringskansliet), *Personal Data Protection: Information on the Personal Data Act*, 4th edition, (Stockholm: Fritzes kundtjänst, 2006) hal.7.
[144] *Id.*, hal.6.

tersebut sah, (ii) tepat dan sesuai dengan praktik-praktik terbaik, (iii) dikumpulkan untuk tujuan khusus, eksplisit dan sah, (iv) tidak diproses melebihi tujuan yang hendak dicapai, (v) data tersebut memadai dan relevan untuk tujuan yang dimaksud, (vi) diperlukan untuk tujuan yang dimaksud, (vii) diproses secara tepat dan jika perlu selalu *up-to-date*, (viii) subjek data berhak untuk memperoleh rektifikasi, memblokir atau menghapus data yang tidak benar atau tidak lengkap, dan (ix) data tersebut tidak disimpan melebihi jangka waktu yang diperlukan.[145]

Sementara itu, jaminan perlindungan terhadap penegakan undang-undang ini, DPA 1998 masih mengakui mandat yang dimiliki *Data inspektionen* (*Data Inspection Board*), sebagaimana ditentukan oleh *Datalag*. Badan ini memiliki kewenangan untuk melakukan pemantauan terhadap praktik pemrosesan data pribadi, hal ini termasuk hak untuk melarang *data controller* beroperasi, menjatuhkan denda, bahkan dapat mengajukan permohonan ke *County Administrative Court* terhadap pelanggaran atas undang-undang ini.[146]

10) Tiongkok (RRT)

Perlindungan data pribadi di RRT dapat dikategorikan terbatas, jika tidak dapat dikatakan tidak terjamin sama sekali, mengingat tidak adanya undang-undang yang secara khusus mengatur tentang perlindungan data pribadi secara umum dan diperparah Pasal 40 Konstitusi RRT[147] tidak memberikan kebebasan mutlak bagi hak atas privasi itu sendiri.

Pengaturan terkait dengan data pribadi dapat ditemukan pula dalam KUHP Tiongkok yang melarang segala macam bentuk penjualan atau penyediaan data pribadi warga negara secara ilegal.[148]Pada praktiknya, hingga tahun 2014 saja pasal ini telah digunakan untuk 260 kasus penuntutan.[149] Akan tetapi, ketentuan ini hanya berlaku bagi organ pemerintah Tiongkok saja, membuat pihak swasta terlepas dari jerat ketentuan ini.[150] Namun, pasca putusan *Zhou Jianping*(2009)[151] dan *Shanghai Roadway* (2012),[152] eksistensi kedua putusan ini jelas merubah penafsiran mengenai ketentuan Pasal 253(a) KUHP Tiongkok tersebut, yang menyebabkan bahwa ketentuan ini berlaku pula bagi pihak swasta maupun perorangan.

Dalam hukum perdata Tiongkok, pengaturan terkait dengan perlindungan data pribadi termanifestasikan setidaknya dalam Pasal 101 KUH Perdata Tiongkok (*General Principles of*

---

[145] *Id.*, hal.15.
[146] *Id.*, hal.27.
[147] RRT, *Constitution*, (1982) Pasal 40.
[148] RRT, *Criminal Law*, (1 Juli 1979) <http://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm> Pasal 253(a).
[149] Scott Livingston dan Graham Greenleaf, "Whys and wherefores – illegal provision under Chinese law", 131 *Privacy L. & Bus. Int'l Rep.* 1 (2014) hal.5.
[150] Paul de Hert dan Vagelis Papakonstantinou, *The Data Protection Regime in China: In-depth Analysis for the LIBE Committee*, (Brussels: European Union, 2015) hal.17-18 [De Hert dan Papakonstantinou].
[151] *Zhou Jianping*, Putusan No. 612 Tahun 2009, (Pengadilan Distrik Xiangzhou, Zhuhai memutuskan bahwa terdakwa bersalah atas pembelian ilegal catatan data telepon milik pejabat tinggi pemerintah Tiongkok yang kemudian dijual kepada penipu (*fraudsters*) yang mengimpersonifikasikan dirinya sebagai pejabat tinggi yang bersangkutan. Zhou dinyatakan bersalah dan dipidana dengan 18 bulan masa penahanan dan berkewajiban untuk membayar sejumlah denda).
[152] Kathy Chu, "Dun & Bradstreet Fined, Four Sentenced in China", Wall Street Journal, (9 Januari 2013) <http://www.wsj.com/articles/SB10001424127887323482504578230781008932240> (Pengadilan Distrik Zhabei, Shanghai memutuskan bahwa Dun & Bradstreet Corp. bertanggungjawab atas pembelian data 150 juta konsumen Tiongkok secara ilegal dan dipidana dengan denda sebesar satu juta Yuan (¥1.000.000,00) serta keempat mantan pejabat eksekutif perusahaan tersebut dipenjara dua tahun).

Civil Law)[153] dan Pasal 2 Undang-Undang Pertanggungjawaban Ganti Rugi (*Tort Liability Law*/*TLL*).[154] Terkait dengan instrumen yang pertama, walaupun tidak secara eksplisit memuat ketentuan terkait hak atas privasi, namun Mahkamah Agung Tiongkok (*Chinese Supreme People's Court*) berpendapat bahwa segala macam bentuk pembukaan informasi pribadi seseorang berpotensi menggangu hak atas reputasi orang yang bersangkutan.[155] Sementara itu, instrumen yang terakhir menekankan bahwa gangguan atau pelanggaran terhadap hak atas privasi seseorang berhak untuk mendapatkan pertanggung-jawaban ganti rugi.[156] Lebih jauh, TLL juga memuat ketentuan bahwa "*network users*" atau "*network service providers*", yang dapat ditafsirkan mencakup pengguna internet dan penyedia jasa internet (*internet service providers*/*ISPs*), dapat dikenakan pertanggungjawaban ganti rugi atas gangguan terhadap privasi seseorang.[157]

Perkembangan pengaturan regulasi terkait perlindungan data pribadi di Tiongkok ini kemudian didukung pula dengan lahirnya keputusan dari *Standing Committee of the National People's Congress* (SC-NPC), organ legislatif tertinggi kedua, yang keputusannya diterima sebagai undang-undang. Pada tahun 2012, SC-NPC menerbitkan Keputusan tentang Perlindungan Informasi Internet (*Decision on Internet Information Protection*/*SC-NPC 2012*).[158] Instrumen yang berisikan 12 pasal ini memiliki tujuan utama untuk melindungi segala macam informasi elektronik, termasuk informasi pribadi.[159] Berdasarkan ketentuan ini, ISPs dan pihak-pihak yang mengumpulkan dan menggunakan informasi pribadi elektronik penduduk Tiongkok dalam menjalankan kegiatannya harus tunduk pada prinsip (i) legalitas, (ii) legitimasi dan kebutuhan, (iii) secara jelas mengindikasikan tujuan yang ingin dicapai, (iv) metode dan cakupan pengumpulan dan penggunaan informasi, dan (v) mendapat persetujuan dari subjek data serta adanya kesepakatan dari kedua belah pihak yang tidak bertentangan dengan ketentuan yang berlaku.[160] SC-NPC 2012 juga mengakui hak-hak subjek data untuk meminta *data controllers* menghapus data, menghentikan gangguan atau melaporkannya kepada *controlling department*, jika ditemukan gangguan terhadap hak subjek data tersebut.[161]

Jika dibandingkan dengan model perlindungan data pribadi ala Eropa, jelas ketentuan ini masih lemah. Pertama, masih terbatasnya cakupan data pribadi yang dilindungi, yakni, hanya sebatas kepada data yang dimuat dalam internet semata. Kedua, prinsip-prinsip yang wajib dipenuhi oleh *data controller* masih belum seutuhnya sesuai dengan prinsip-prinsip yang diterapkan di kawasan Eropa. Ketiga, tidak adanya mekanisme penegakan yang memberikan mandat kepada institusi khusus untuk melakukan supervisi. Pula, eksistensi *controlling department* sebagaimana dimaksud dalam Pasal 9 dan 10 SC-NPC 2012 dinilai masih belum jelas secara praktiknya.[162]

---

[153] RRT, *General Principles of Civil Law*, (1986) Pasal 101.
[154] RRT, *Tort Liability Law*, (2009) Pasal 2 [TLL].
[155] De Hert dan Papakonstantinou, *Op.Cit.*, hal.18.
[156] Yuanshi Bu (ed.), *Chinese Civil Law*, (Munchen: C.H. Beck, 2013) hal.143.
[157] TLL, *Op.Cit.*, hal.19.
[158] RRT, *SC-NPC Decision on Internet Information Protection*, (2012) <https://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/> [SC-NPC 2012].
[159] *Id.*, Pasal 1.
[160] *Id.*, Pasal 2.
[161] *Id.*, Pasal 8-9.
[162] Lihat kritisasi terhadap SC-NPC 2012 dalam De Hert dan Papakonstantinou, *Op.Cit.*, hal.20.

Instrumen lain yang perlu menjadi sorotan terkait dengan pengaturan perlindungan data pribadi di RRT adalah *Amendments to the Law on the Protection of Consumer Rights and Interests* oleh SC-NPC pada tahun 2013. Intinya, sebagai bagian harmonisasi dari SC-NPC 2012, ketentuan terkait dengan perlindungan terhadap konsumen juga mencakup kepada aspek perlindungan atas data pribadi konsumen itu sendiri.[163]

Lebih jauh, di tingkat kementerian, khususnya Kementerian Industri dan Teknologi Informasi (*Ministry of Industry and Information Technology*/*MIIT*), setidaknya terdapat tiga instrumen yang dapat menjadi acuan untuk melindungi data pribadi, yaitu:[164] (i) *MIIT Regulations* 2011,[165] (ii) *MIIT Guidelines 2013*[166] dan (iii) *MIIT Regulations 2013*.[167] Secara substansial, pembentukan regulasi dan panduan ini banyak mengabsorpsi nilai-nilai perlindungan terhadap hak atas privasi setiap individu sebagaimana tertuang dalam *OECD Guidelines*.[168]

Tegasnya, upaya perlindungan data pribadi yang beragamdalam praktik di sejumlah negara seperti terurai *supra* dapat ditemukan suatu benang merah bahwa kesepuluh negara di atas menyadari pentingnya eksistensi regulasi dan mekanisme penegakan terhadap regulasi tersebut. Oleh karena itu, tabel berikut ini akan meringkaskan perbandingan perlindungan data pribadi yang ada pada sepuluh negara tersebut.

Tabel 2: **Perbandingan Perlindungan Data Pribadi di Beberapa Negara**

NEGARA	INSTRUMEN HUKUM	BADAN PENGAWAS
Afrika Selatan	*Protection of Personal Information Act 2013* (POPI)	*Information Regulator*
Amerika Serikat	*Privacy Act 1974*	- *Office of Management and Budget* (OMB) - *Data Integrity Boards* yang ada dalam setiap agen federal
Filipina	*Data Privacy Act 2012* (DPA)	*National Privacy Commission*
Inggris	*Data Protection Act 1998* (DPA)	*Information Commissioner's Office* (ICO)
Jepang	*Act on the Protection of Personal Information 2003* (APPI)	*Privacy Information Protection Commission* (PIPC)
Jerman	*Federal Data Protection Act 1977* (FDPA)	*Federal Commissioner for Data Protection and Freedom of Information* (BfDI)

[163] De Hert dan Papakonstantinou, *Op.Cit.*, hal.22.
[164] Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives*, (Oxford: Oxford University Press, 2014) hal.14.
[165] RRT, *MIIT Regulations on Standarizing Market Order for Internet Information Services*, (7 Desember 2011).
[166] RRT, *MIIT Guidelines for Personal Information Protection within Public and Commercial Services Information Systems*, (21 Januari 2013).
[167] RRT, *MIIT Telecommunications and Internet Personal User Data Protection Regulations*, (28 Juni 2013).
[168] De Hert dan Papakonstantinou, *Op.Cit.*, hal.20.

Malaysia	*Personal Data Protection Act 2010* (PDPA)	*Personal Data Protection Commissioner*
Prancis	*Law on Computers, Files and Freedoms 1978*	*National Commission on Informatics and Liberty* (CNIL)
Swedia	*Personal Data Act 1998* (PDA 1998)	*Data Inspection Board*
RRT	*SC-NPC Decision on Internet Information Protection 2012*	-

Berdasarkan praktik di sepuluh negara tersebut dapat dipahami bahwa pada umumnya semua negara ini telah memiliki medium pengaturan terkait perlindungan data pribadi, terlepas kesempurnaan materi muatan yang diatur dalam undang-undang di setiap negara. Sementara itu dari segi penegakan hukumnya, tidak semua negara memiliki institusi khusus yang memiliki kewenangan untuk melakukan supervisi. Setidaknya, hingga tulisan ini diterbitkan tiga dari sepuluh negara tersebut secara *de facto* belum mempunyai alat kelengkapan untuk memantau pengimplementasian perlindungan data pribadi. Afrika Selatan dan Jepang, sekalipun telah memandatkan suatu badan tertentu untuk melakukan supervisi, namun pada praktiknya badan tersebut belum eksis berdiri. Sementara di RRT, justru tidak ada institusi sama sekali yang memiliki kewenangan supervisi tersebut.

D.3. Cakupan perlindungan data pribadi

Merujuk kepada sejumlah instrumen internasional di atas, serta praktik-praktik di beberapa negara tersebut, berikut ini diuraikan cakupan-cakupan perlindungan data pribadi dalam instrumen-instrumen tersebut, *inter alia*, ICCPR, *OECD Guidelines*, *APEC Privacy Framework*, *DP Directive* dan praktik di Amerika Serikat.

Sebagai suatu hak yang dilindungi dalam kerangka HAM, perlindungan data pribadi tidak terlepas dari pembatasan yang mungkin diberikan mengingat hak atas privasi dalam konteks privasi informasi tidak masuk ke dalam kategori hak yang tidak dapat dikurangi (*non-derogable rights*) pada Pasal 4 ayat (1) ICCPR. Akan tetapi, Pasal 17 tersebut tidak secara tegas menentukan batasan-batasan yang dapat digunakan untuk hak atas privasi ini. Untuk itu, Pelapor Khusus Frank La Rue menyampaikan dalam laporannya bahwa pembatasan terhadap ketentuan ini dapat merujuk pada Komentar Umum 27[169] yang mensyaratkan pembatasan dimungkinkan jika memenuhi elemen berikut ini:[170]

1) Segala bentuk pembatasan harus diatur dengan undang-undang;
2) Pembatasan tidak boleh melanggar esensi perlindungan HAM;
3) Pembatasan dilakukan dalam masyarakat yang demokratis;
4) Setiap kebijakan pembatasan tidak boleh mengekang pelaksanaan hak tersebut;
5) Pembatasan yang dibolehkan tidak cukup ditujukan hanya untuk mencapai tujuan yang sah, tetapi juga harus benar-benar dibutuhkan untuk melindungi tujuan tersebut; dan

[169] UN Doc.CCPR/C/21/Rev.1/Add.9 (1999) para.11-15.
[170] UN Doc.A/HRC/23/40 (2013) para.28-29.

6) Pembatasan harus sesuai dengan prinsip proporsionalitas, yakni sesuai untuk mencapai fungsi perlindungan, harus menjadi instrumen yang tidak sangat intrusif sehingga memungkinkan mencapai hasil yang diinginkan, dan proporsional dengan kepentingan yang harus dilindungi.

Berdasarkan *OECD Guidelines*, cakupan perlindungan yang diberikan dalam pedoman ini berlaku bagi data pribadi, baik yang berada pada sektor publik atau privat, yang karena pemrosesan, sifat atau konteks penggunaannya, membahayakan privasi dan kebebasan seseorang.[171] Pengecualian terhadap perlindungan data pribadi dalam pedoman ini juga dimungkinkan atas dasar kedaulatan nasional, keamanan nasional dan kebijakan publik ("*ordre public*") sepanjang dilakukan sesedikit mungkin dan harus diketahui publik.[172]

APEC Privacy Framework menegaskan bahwa instrumen ini hanya berlaku bagi data yang dapat digunakan atau dengan dukungan data lain dapat mengidentifikasikan seseorang.[173] Pelaksanaan terhadap prinsip-prinsip yang tertuang dalam instrumen ini harus diterapkan secara fleksibel dengan mempertimbangkan limitasi-limitasi terhadap prinsip tersebut atas dasar proporsionalitas untuk mencapai tujuan yang dimaksud, dan diketahui publik atau sesuai dengan hukum.[174]

Sementara itu *DP Directive* membatasi ruang lingkupnya sebatas pada pemrosesan data pribadi, baik secara keseluruhan ataupun sebagian dengan alat otomatis, serta pada kegiatan pengolahan data pribadi yang dilakukan oleh seseorang dalam kegiatan murni untuk kepentingan pribadi. Ketentuan ini juga menegaskan mengenai status keberlakuannya yang tidak dapat diterapkan pada hal keamanan nasional dan undang-undang tindak pidana.[175]

Berbeda dengan di daratan Eropa, cakupan perlindungan data pribadi di Amerika Serikat cenderung bersifat meluas, mengingat tidak adanya instrumen hukum yang secara khusus menjadi payung bagi perlindungan data pribadi. Untuk dapat memahami karakteristik data pribadi yang dilindungi, Paul M. Schwarz dan Daniel J. Solove membagi setidaknya tiga pendekatan yang dapat digunakan untuk menafsirkan jenis data pribadi yang dapat dilindungi, yakni pendekatan tautologikal, pendekatan non-publik dan pendekatan khusus.[176]

Dalam pendekatan tautologikal, data pribadi yang dilindungi hanyalah sebatas kepada data atau informasi yang mengidentifikasikan seseorang. Hal ini tercermin dalam pengaturan pada VPPA yang mendefinisikan "*personally identifiable information*" sebagai "informasi yang mengidentifikasikan individu".[177]

Sementara pendekatan non-publik menafsirkan perlindungan data pribadi hanya berlaku kepada data yang tidak dapat diakses oleh publik. Ketentuan terkait dengan pendekatan ini adalah GLBA, akan tetapi instrumen ini tidak mengelaborasi lebih lanjut terkait rasio dari

[171] *OECD Guidelines*, *Op.Cit.*, para.2.
[172] *Id.*, para.4.
[173] *APEC Privacy Framework*, *Op.Cit.*, penjelasan para.9.
[174] *Id.*, para.12-13.
[175] Edmon Makarim, *Op.Cit.*, hal.167.
[176] Schwartz dan Solove (2011), *Op.Cit.*, hal.1828-1836.
[177] Schwartz dan Solove (2014), *Op.Cit.*, hal.888.

pendekatan jenis ini, tetapi hanya menegaskan bahwa "*personally identifiable financial information*" sebagai informasi personal non-publik.[178]

Pendekatan ketiga atau "*specific type approach*" menekankan pentingnya suatu daftar khusus yang dapat dijadikan rujukan yang berisikan bentuk-bentuk atau jenis-jenis data yang dapat dikualifisir sebagai data pribadi yang patut untuk dilindungi. Hal nampak pada *Section 1 Massachusetts General Law Chapter 39H* yang menyebutkan data pribadi mencakup pada nama depan dan belakang seseorang, atau inisial nama depan dan belakang yang dikombinasikan dengan nomor jaminan sosial, nomor surat izin mengemudi, nomor akun keuangan, baik debit maupun kredit, seseorang.[179]

D.4. Pengawasan terhadap perlindungan data pribadi

Pasal 17 ayat (2) ICCPR dengan tegas menyatakan bahwa setiap orang memiliki hak atas perlindungan hukum terhadap campur tangan atau serangan yang tidak sah atau sewenang-wenang. Konsep "perlindungan hukum" tersebut harus diberikan secara langsung melalui prosedur pengamanan yang efektif, termasuk melalui pengaturan sumber daya kelembagaan yang memadai. Praktik di sejumlah negara memperlihatkan bahwa salah satu strategi yang diterapkan dalam melindungi data pribadi penduduk adalah dengan membentuk suatu badan pengawasan khusus terhadap pengelolaan data pribadi oleh pihak ketiga.

Akan tetapi, menurut Pelapor Khusus PBB lemahnya mekanisme pemantauan yang efektif berkontribusi bagi rendahnya akuntabilitas terhadap serangan yang sewenang-wenang atau tidak sah bagi hak atas privasi. Institusi pengawasan internal yang tidak didukung dengan independensi, telah terbukti pula tidak efektif dalam menghadapi praktik pemindaian yang tidak sah dan sewenang-wenang. Meskipun mekanisme pemantauan ini dapat menggunakan beragam bentuk, keterlibatan semua lembaga kepemerintahan dalam mengawasi program pemindaian, di dukung dengan adanya badan pengawasan sipil yang independen, menjadi hal yang esensial dalam menjamin efektivitas perlindungan hukum bagi penikmat hak atas privasi tersebut.[180]

Bahkan, hal ini ditegaskan pula oleh Majelis Umum PBB (*UN General Assembly*) melalui Resolusi Majelis Umum 68/167 di tahun 2014. Resolusi ini menyerukan kepada semua negara anggota PBB untuk mendirikan atau mempertahankan suatu badan supervisi independen yang efektif di tingkat nasional yang memiliki mandat untuk menjamin transparansi, yang sesuai, dan pertanggungjawaban atas *surveillance* komunikasi, intersepsi dan pengumpulan data pribadi yang dilakukan oleh aparatur negara.[181]

Lebih jauh, di tingkat regional pun penekanan akan pentingnya eksistensi mekanisme pengawasan seperti ini menjadi hal yang tak terbantahkan. Mahkamah Eropa (*European Court of Justice*/CJEU) mengafirmasi dalam diktumnya pada beberapa kasus bahwa intervensi

[178] *Id.*, hal.889.
[179] *Id.*, hal.889-890.
[180] UN Doc.A/HRC/27/37 (2014) para.37.
[181] *The right to privacy in the digital age*, Resolusi Majelis Umum 68/167, UN Doc.A/RES/68/167 (2014) para.4(d) [Resolusi 68/167].

pemerintah, baik secara langsung maupun tidak langsung, terhadap kinerja kerja lembaga pengawasan dapat memperlemah independensi institusi itu sendiri.[182]

D.5. Mekanisme pemulihan yang disediakan jika terjadi pelanggaran

ICCPR mewajibkan setiap negara pihak untuk menjamin korban yang haknya terlanggarkan dalam Kovenan ini mendapatkan pemulihan yang efektif (*effective remedy*). Bahkan secara khusus pada Pasal 2 ayat 3(b) secara khusus menyatakan:

> "*Setiap Negara Pihak pada Kovenan ini berjanji (...) menjamin, bahwa setiap orang yang menuntut upaya pemulihan tersebut harus ditentukan hak-haknya itu oleh lembaga peradilan, administratif atau legislatif yang berwenang, atau oleh lembaga berwenang lainnya yang diatur oleh sistem hukum negara tersebut, dan untuk mengembangkan segala kemungkinan upaya penyelesaian peradilan.*"

Dalam konteks ini negara berkewajiban untuk memastikan otoritas yang berwenang tersebut untuk memberikan pemulihan yang dimohonkan, apabila diterima otoritas penyelesaian sengketa yang berwenang. Sebagaimana ditekankan oleh Komite HAM PBB pada Komentar Umum 31 ICCPR, kegagalan negara pihak untuk melakukan investigasi terhadap indikasi pelanggaran HAM yang termuat dalam Kovenan dapat dengan sendirinya dikategorikan sebagai bentuk lain dari pelanggaran ICCPR, disamping pelanggaran terhadap hak yang bersangkutan. Pada intinya, penghentian (*cessation*) terhadap pelanggaran yang tengah terjadi merupakan syarat mutlak bagi terpenuhi pemulihan yang efektif tersebut.[183]

Pemulihan efektif bagi pelanggaran hak atas privasi dalam hal perlindungan data pribadi kemudian dapat menggunakan mekanisme yudisial, legislatif atau pun administratif. Setidaknya Pelapor Khusus PBB mencatat bahwa pemulihan yang efektif harus memenuhi empat karakteristik dasar, yaitu:[184]

1) Pemulihan tersebut harus diketahui dan dapat diakses oleh semua orang yang merasa haknya terlanggarkan;
2) Pemulihan yang efektif pasti akan melalui proses investigasi yang cepat, menyeluruh dan tidak memihak;
3) Mekanisme pemulihan ini harus mampu untuk mengakhiri pelanggaran yang tengah berlangsung tersebut; dan
4) Ketika pelanggaran HAM tersebut meningkat eskalasinya menjadi pelanggaran berat, maka mekanisme pemulihan non-yudisial tidak dapat digunakan, sehingga hal ini akan menempatkan penuntutan secara pidana pun dengan serta merta mutlak berlaku.

---

[182] Lihat *European Commission v. Federal Repulic of Germany*, C-518/07, Ct.J.E.U. (2010) para.27; *European Commission v. Repulic of Austria*, C-614/10, Ct.J.E.U. (2012) para.59,63.
[183] UN Doc.CCPR/C/21/Rev.1/Add.13 (2004) para.15.
[184] UN Doc.A/HRC/27/37 (2014) para.40-41.

E. GAMBARAN UMUM REGULASI PERLINDUNGAN DATA PRIBADI DI INDONESIA

Perkembangan teknologi yang semakin canggih menimbulkan sejumlah tantangan baru khususnya dalam hal penikmatan hak atas privasi. Pemenuhan kebutuhan yang menggunakan teknologi internet yang berbasis data semakin menjamur di Indonesia. Mulai dari bidang perbankan, kesehatan, transaksi perdagangan, bahkan transportasi *online* atau berbagai kegiatan lain yang memerlukan pengumpulan data pribadi. Fenomena tersebut menimbulkan tantangan tersendiri khususnya menghadapi permasalahan jaminan perlindungan data pribadi.

Dalam tingkat ekonomi global, Indonesia dinilai sebagai negara dengan posisi strategis dalam perdagangan internasional, termasuk transaksi elektronik yang memungkinkan terjadinya persebaran data pribadi yang semakin luas.[185] Namun pada kenyataannya, Indonesia merupakan salah satu negara di ASEAN yangmasih belum memiliki kebijakan atau regulasi yang secara khusus mengenai perlindungan data pribadi.[186]

Kendati demikian, dalam menakar jaminan perlindungan hukum terkait dengan data pribadi setidaknya Konstitusi Indonesia dan sejumlah perundang-undangan sektoral telah berupaya memberikan jaminan yang dimaksud. Untuk dapat memahami hal tersebut, berikut ini akan disajikan uraian pengaturan data pribadi dalam instrumen-instrumen hukum yang telah disebutkan itu.

E.1. Jaminan konstitusi perlindungan data pribadi

Seperti yang telah disebutkan pada bab sebelumnya, perlindungan data pribadi merupakan salah satu bentuk penghormatan terhadap hak atas privasi. Meskipun Indonesia belum memiliki peraturan *lex specialis* yang mengatur tentang perlindungan data pribadi, tetapi jaminan perlindungan akan hak privasi termuat dalam konstitusi Indonesia, yaitu Undang-Undang Dasar Negara Republik Indonesia 1945 (UUD 1945), khususnya Pasal 28G yang berbunyi:

> "*Setiap orang berhak atas perlindungan atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.*"

Berdasarkan ketentuan tersebut, UUD 1945 tidak secara eksplisit menyebut mengenai privasi dan perlindungan data pribadi. Namun sebagai konstitusi negara, yang menjadi rekomendasi kuat dalam melindungi HAM, pasal tersebut dapat menjadi rujukan untuk membentuk peraturan yang lebih khusus mengenai perlindungan data pribadi.

---

[185] Heppy Endah Palupy, *Privacy and Data Protection: Indonesia Legal Framework*, Tesis Program Master Law and Technology di Universiteit van Tilburg, Tilburg (2011) hal.35.

[186] Yoga Hastyadi Widiartanto, "Indonesia Belum Punya UU Perlindungan Data Pribadi", Kompas, (17 Februari 2015) <http://tekno.kompas.com/read/2015/02/17/09544927/indonesia.belum.punya.uu. perlindungan.data.pribadi>.

E.2. Jaminan perlindungan data pribadi dalam peraturan perundang-undangan

Meskipun belum dituangkan dalam peraturan khusus mengenai perlindungan data pribadi,[187] jaminan akan perlindungan data pribadi atau setidaknya bersinggungan dengan aspek data pribadi, sesungguhnya telah tertuang dalam beberapa peraturan perundang-undangan di Indonesia, *inter alia*:

1) Undang-Undang No. 1 Tahun 1946 tentang Kitab Undang-Undang Hukum Pidana (KUHP);
2) Undang-Undang No. 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP);
3) Undang-Undang No. 8 Tahun 1997 tentang Dokumen Perusahaan (UU Dokumen Perusahaan);
4) Undang-Undang No. 10 Tahun 1998 tentang Perbankan (UU Perbankan);
5) Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK);
6) Undang-Undang No. 23 Tahun 1999 tentang Bank Indonesia (UU BI);
7) Undang-Undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi (UU Tipikor);
8) Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi);
9) Undang-Undang No. 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM);
10) Undang-Undang No. 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi (UU KPK);
11) Undang-Undang No. 15 Tahun 2003 tentang Penetapan Perppu No. 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme (UU Anti-Terorisme);
12) Undang-Undang No. 18 Tahun 2003 tentang Advokat (UU Advokat);
13) Undang-Undang No. 29 Tahun 2004 tentang Praktik Kedokteran (UU Praktik Kedokteran);
14) Undang-Undang No. 23 Tahun 2006 tentang Administrasi Kependudukan (UU Adminduk);
15) Undang-Undang No. 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang (UU TPPO);
16) Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE);
17) Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP);
18) Undang-Undang No. 21 Tahun 2008 tentang Perbankan Syariah (UU Perbankan Syariah);
19) Undang-Undang No. 35 Tahun 2009 tentang Narkotika (UU Narkotika);
20) Undang-Undang No. 36 Tahun 2009 tentang Kesehatan (UU Kesehatan);
21) Undang-Undang No. 43 Tahun 2009 tentang Kearsipan (UU Kearsipan);
22) Undang-Undang No. 44 Tahun 2009 tentang Rumah Sakit (UU Rumah Sakit);
23) Undang-Undang No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU);
24) Undang-Undang No. 17 Tahun 2011 tentang Intelijen Negara (UU Intelijen Negara);
25) Undang-Undang No. 18 Tahun 2011 tentang Perubahan Undang-Undang No. 22 Tahun 2004 tentang Komisi Yudisial (UU KY);
26) Undang-Undang No. 21 Tahun 2011 tentang Otoritas Jasa Keuangan (UU OJK);

[187] Edmon Makarim, *Op.Cit.*, hal.177.

27) Undang-Undang No. 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme (UU Pendanaan Terorisme);
28) Undang-Undang No. 7 Tahun 2014 tentang Perdagangan (UU Perdagangan);
29) Undang-Undang No. 18 Tahun 2014 tentang Kesehatan Jiwa (UU Kesehatan Jiwa); dan
30) Undang-Undang No. 36 Tahun 2014 tentang Tenaga Kesehatan (UU Tenaga Kesehatan).

Dalam hal ini, maka kumpulan peraturan perundang-undangan tersebutdi atas idealnya harus dipandang sebagai landasan pembentukan kerangka hukum perlindungan data pribadi di Indonesia. Berikut ini akan diuraikan mengenai materi muatan yang diatur dalam ketiga puluh undang-undang tersebut di atas.

1) Undang-Undang No. 1 Tahun 1946 (KUHP)

Perlindungan data pribadi dalam KUHP tertuang dalam Bab XXVIII tentang Kejahatan Jabatan, terutama pada Pasal 430-433. Secara umum, muatan pasal tersebut mengatur tentang kewajiban untuk menjaga kerahasiaan bagi pegawai negeri yang aktivitasnya berkaitan dengan data pribadi seperti surat, telepon, telegram, barang atau paket milik orang lain.

Misalnya, dalam Pasal 430 ayat (1) disebutkan bahwa pegawai negeri dinyatakan melampaui kekuasaan ketika dirinya menyuruh memperlihatkan kepadanya, merampas surat, kartu pos, barang atau paket yang dikirim melalui perusahaan pengangkutan umum. Atas tindakan tersebut, pegawai negeri diancam pidana paling lama dua tahun delapan bulan. Demikian pula untuk tindakan melampaui kewenangan bagi pegawai negeri atau pihak yang ditugaskan dalam bidang telekomunikasi untuk kepentingan umum, kemudian dipaksa untuk memberikan keterangan kepadanya.

Dalam Pasal 431 juga disebutkan bahwa pegawai negeri suatu lembaga pengangkutan akan diancam pidana penjara jika dengan sengaja dan melawan hukum membuka atau memeriksa surat, barang tertutup atau paket milik orang lain, kemudian memberitahukannya kepada orang lain diancam pidana penjara paling lama dua tahun, sedangkan Pasal 432 KUHP mengatur mengenai pengawai negeri yang bekerja dalam lembaga pegangkutan umum dengan sengaja memberikan hak kepada orang lain untuk mengakses data pribadi milik orang lain, menghancurkan, menghilangkan, atau memiliki sendiri, mengubah isi diancam pidana penjara paling lama lima tahun. Sementara itu, Pasal 433 KUHPmenyebutkan secara khusus tentang pegawai negeri yang memiliki wewenang untuk mengawasi aktivitas pengguna teknologi telepon dapat diancam pidana penjara bila membocorkan isi percakapan kepada orang lain, atau menghancurkan dan mengubahnya secara sepihak.

Meski tidak dirumuskan secara eksplisit dalam pasal, rumusan diatas menunjukkan KUHP memiliki perhatian khusus dalam hal perlindungan data pribadi. Hal tersebut terlihat dari adanya ancaman pidana untuk setiap pelanggaran pengelolaan data pribadi terutama bagi pegawai negeri yang memiliki tugas dan wewenang untuk mengaksesnya.

2) Undang-Undang No. 8 Tahun 1981 (KUHAP)

Berdasarkan Pasal 47 KUHAP, Polisi memiliki kewenangan untuk mengakses surat pribadi seseorang yang dikirim melalui kantor pos termasuk informasi melalui teknologi

telekomunikasi. Kewenangan tersebut harus melalui prosedur pemberian izin khusus dari ketua Pengadilan Negeri. Pemberian izin seperti ini menunjukkan adanya suatu bentuk pengawasan *pre facto* atau pengawasan sebelum intersepsi tersebut dilakukan.[188] Selain itu, akses terhadap surat pribadi juga dibatasi hanya terhadap surat pribadi yang dicurigai dengan alasan kuat mempunyai hubungan dengan perkara pidana yang sedang diperiksa.

Meskipun ketentuan dalam KUHAP ini mengizinkan adanya pelanggaran terhadap hak atas privasi seseorang. Akan tetapi, pasal tersebut juga memberikan perlindungan data pribadi terhadap pemegang hak yang terlihat dari prosedur yang mewajibkan akses data pribadi harus melalui izin khusus peradilan dan adanya pembatasan akses terhadap data-data tertentu saja.

3) Undang-Undang No. 8 Tahun 1997 (UU Dokumen Perusahaan)

Pada dasarnya UU Dokumen Perusahaan ditujukan untuk melengkapi ketentuan mengenai pokok kearsipan yang lebih banyak mengatur aspek publik, dalam lingkup perusahaan. Berdasarkan Pasal 1 UU tersebut, terminologi dokumen perusahaan diartikan sebagai data, catatan dan atau keterangan yang dibuat dan atau diterima oleh perusahaan dalam rangka pelaksanaan kegiatannya baik tertulis di atas kerta atau sarana lain maupun terekam dalam bentuk corak apa pun yang dapat dilihat, dibaca atau didengar. Sedangkan berdasarkan jenisnya, Pasal 2 UU Dokumen Perusahaan secara tegas menglasifikasikan dokumen perusahaan yang terdiri dari dokumen keuangan dan dokumen lainnya.[189] Macam-macam varian dari dokumen lainnya dapat mencakup data pelanggan dan data karyawan yang sudah sepatutnya tergolong ke dalam data pribadi.

Sehubungan dengan hal tersebut, undang-undang ini mengizinkan suatu perusahaan untuk melakukan penyimpanan atas dokumen lain tersebut berdasarkan jadwal retensi yang telah ditetapkan oleh pimpinan perusahaan;[190] yang rentan durasi masa penyimpanannya tidak sekalipun mempengaruhi fungsi dokumen tersebut sebagai alat bukti, kaitannya dengan ketentuan daluwarsa suatu tuntutan.[191]

Selain itu, dokumen perusahaan juga dimungkinkan untuk dipindahtangankan kepada Arsip Nasional Republik Indonesia (ANRI) berdasarkan keputusan pimpinan perusahaan, sepanjang dokumen tersebut memiliki nilai guna bagi kepentingan nasional.[192] Dalam hal pemusnahan data, UU Dokumen Perusahaan menegaskan bahwa hal tersebut dapat dilakukan berdasarkan jadwal retensi yang telah ditetapkan sebelumnya.[193] Pasca pelaksanaan hal itu, perusahaan berkewajiban untuk membuat suatu berita acara khusus perihal pemusnahan tersebut.[194]

4) Undang-Undang No. 10 Tahun 1998 (UU Perbankan)

UU Perbankan,yang merupakan upaya pemerintah untuk memberikan kepastian hukum dalam kegiatan perbankan, mengatur mengenai sederet permasalahan perbankan secara

---

[188] Reda Manthovani, *Penyadapan vs. Privasi*, (Jakarta: Bhuana Ilmu Populer, 2013) hal.299 [Manthovani].
[189] Pasal 4 UU Dokumen Perusahaan mendefinisikan "dokumen lainnya" sebagai data atau setiap tulisan yang berisi terkait keterangan yang mempunyai nilai guna perusahaan meskipun tidak terkait langsung dengan dokumen keuangan.
[190] Pasal 11 ayat (3)-(4) UU Dokumen Perusahaan.
[191] *Id.*, Pasal 11 ayat (5).
[192] *Id.*, Pasal 18 ayat (1).
[193] *Id.*, Pasal 19 ayat (2).
[194] *Id.*, Pasal 21.

kelembagaan, termasuk mengenai permasalahan kerahasiaan bank (*bank secrecy*), dengan berlandaskan prinsip kerahasiaan (*confidential principle*),yang mewajibkan bank untuk merahasiakan segala sesuatu yang berhubungan dengan data dan informasi mengenai nasabah, baik keadaan keuangannya maupun informasi yang bersifat pribadi.[195]

Dalam Pasal 1 ayat (28) UU Perbankan, rahasia bank ditafsirkan sebagai segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya. Dengan demikian, asas kepercayaan dan kerahasiaan sebagai landasan kinerja lembaga keuangan, turut diterapkan dalam hubungan antara pihak nasabah dan bank. Nasabah dalam melakukan penyimpanan atau menggunakan produk bank lainnya harus memberikan data pribadi yang dianggap perlu kepada bank. Hubungan tersebut harus didukung dengan kemampuan pihak bank dalam menjaga kepercayaan nasabah serta melindungi privasi dari nasabah yang telah memberikan dan memercayakan data pribadinya. Hal tersebut tertuang dalam Pasal 40 UU Perbankan yang menyebutkan bahwa bank berkewajiban untuk merahasiakan keterangan mengenai nasabah penyimpanan dan simpanannya, kecuali dalam hal-hal tertentu yang dibolehkan. Pengaturan tersebut mengisyaratkan perlindungan privasi nasabah tidak hanya berkenaan dengan data keuangan (simpanan atau produk bank lain) miliknya tetapi juga mengenai data pribadi nasabah yang bersifat informasi ataupun keterangan yang menyangkut identitas atau data pribadi lain di luar data keuangan. Kewajiban ini diperkuat dengan hadirnya Pasal 47 ayat (2) yang menegaskan adanya ancaman pidana penjara paling rendah 2 tahun dan denda sebesar empat milyar hingga delapan milyar rupiah (Rp4.000.000.000,00-Rp8.000.000.000,00).

Dalam hal tersebut, Pasal 29 ayat (1) UU Perbankan bahkan mengatur bahwa lembaga yang berwenang mengawas aktivitas bank, termasuk menjaga kerahasiaan bank sepenuhnya berada di bawah mandat Bank Indonesia (BI). Ketentuan ini berlaku setidaknya sampai berdirinya Otoritas Jasa Keuangan (OJK) yang dibentuk berdasarkan UU OJK.

5) Undang-Undang No. 8 Tahun 1999 (UUPK)

Praktik perdagangan dewasa ini menunjukkan bahwa data pribadi mengenai konsumen sering kali didapatkan ketika konsumen menggunakan jasa atau membeli suatu barang. Sebagai contoh pada saat transaksi dengan cara *online*, konsumen harus memberikan informasi diri untuk memenuhi proses transaksi.[196] Data-data yang didapatkan pelaku usaha kemudian disalahgunakan untuk kepentingan tertentu.[197]

Akan tetapi, ironisnya jaminan perlindungan terhadap data/informasi konsumen yang diakui dalam UU Perbankan tidak diikuti pula oleh UUPK. Instrumen ini hanya mengatur mengenai perlindungan terhadap data/informasi barang dan jasa semata,sebagaimana tercermin pada Pasal 9 ayat (1) UUPK yang melarang kegiatan untuk menawarkan, memproduksikan, mengiklankan suatu barang dan/atau jasa secara tidak benar. Walaupun UUPK juga menjatuhi

---

[195] Djoni S. Gazali dan Rachmadi Usman, *Hukum Perbankan*, (Jakarta: Sinar Grafika, 2010) hal.30.

[196] Bambang Pratama, "Perlindungan Data Pribadi pada Pemesanan Transportasi Online Sejenis Go-Jek", Rubrik Universitas Bina Nusantara (Agustus 2015) <http://business-law.binus.ac.id/2015/09/12/ perlindungan-data-pribadi-pada-pemesanan-transportasi-online-sejenis-go-jek/>.

[197] Lihat contoh Daniel Gunawan, "Pengguna Go-Jek Diteror Setelah memberikan *Bad Review*!", Tech in Asia, (3 September 2015) <https://id.techinasia.com/talk/pengguna-go-jek-diteror-setelah-memberikan-bad-review/>; Audi Eka Prasetyo, "Apa yang Harus Go-Jek dan *Startup* Transportasi Lainnya Lakukan untuk Melindungi Privasi Pengguna", Tech in Asia, (15 September 2015) <https://id.techinasia.com/talk/ privasi-pengguna-go-jek/>.

sanksi pidana atas pelanggaran terhadap ketentuan tersebut, namun hal ini masih belum mengakomodir pemulihan bagi korban atau konsumen yang data pribadinya terlanggarkan melalui praktik jual-beli data konsumen secara langsung.

6) Undang-Undang No. 23 Tahun 1999 (UU BI)

Seperti halnya UU Perbankan dan UU Perbankan Syariah, Pasal 24 dan 27 UU BI memperkokoh pengakuan terhadap kewenangan BI untuk melakukan pengawasan terhadap kegiatan perbankan,[198] termasuk hal-hal yang bersinggungan dengan pembukaan data pribadi nasabah oleh pihak bank, sampai dibentuknya lembaga independen yang secara khusus melakukan kegiatan pengawasan.[199] Undang-undang ini juga memungkinkan BI untuk melimpahkan kewenangan pemantauan ini kepada pihak lain yang bertindak atas nama BI untuk melakukan pemeriksaan kepada bank terperiksa dengan tetap menjamin unsur kerahasiaan data yang diperoleh selama masa pemeriksaan tersebut.[200]

7) Undang-Undang No. 31 Tahun 1999 (UU Tipikor)

Sejak era reformasi upaya pemberantasan tindak pidana korupsi semakin menguat. Salah satunya dari segi hukum, sejumlah peraturan perundang-undangan dibentuk untuk memperkuat upaya penegakan hukum tindak pidana korupsi. Penguatan tersebut terlihat dari kewenangan khusus yang diberikan kepada Komisi Pemberantasan Korupsi (KPK). Tidak jarang kewenangan khusus tadi bersinggungan dengan hak privasi pihak pihak yang diduga kuat sebagai pelaku korupsi. Dalam penjelasan Pasal 26 menyebutkan bahwa dalam proses penyidikan, penuntutan dan pemeriksaan kasus korupsi, penyidik memiliki kewenangan penyadapan (*wiretapping).*

Selain penyadapan, pembatasan terhadap hak privasi juga terlihat dalam Pasal 28, 29 dan 30 UU Tipikor. Dalam Pasal 28 disebutkan kewajiban tersangka untuk memberikan keterangan terkait harta benda keluarganya termasuk istri dan anak serta korporasi miliknya. Demikian pula dalam Pasal 29, pihak bank dapat dimintai keterangan terkait data pribadi kekayaan tersangka. Bahkan, dalam ayat (4) pasal tersebut disebutkan bahwa aparat penegak hukum seperti penyidik, penuntut umum, atau hakim dapat meminta pihak bank untuk memblokir rekening simpanan milik tersangka. Pasal 30 juga memberikan kewenangan bagi penyidik untuk membuka, memeriksa, dan menyita surat serta kiriman melalui pos atau alat komunikasi lain milik tersangka. Seluruh kewenangan tersebut dilakukan oleh penyidik berdasarkan bukti yang cukup dan hanya yang dicurigai berhubungan dengan perkara kejahatan korupsi yang dimaksud.

Terkait perlindungan data pribadi, UU Tipikor tidak membahas detil mekanisme yang berkaitan dengan privasi tersangka atau keluarga tersangka pelaku tindak kejahatan. Tetapi dalam hal kerahasiaan identitas pelapor, undang-undang ini menegaskan bahwa saksi dan orang lain dalam proses persidangan dilarang menyebutkan data seperti nama, alamat atau hal yang membuka kemungkinan terbongkarnya identitas pelapor.[201]

---

[198] Lihat pula Peraturan Bank Indonesia (PBI) No. 2/19/PBI/2000 tentang Persyaratan dan Tata Cara Pemberian Perintah atau Izin Tertulis Membuka Rahasia Bank.

[199] Pasal 34-35 UU BI.

[200] *Id.*, Pasal 30 ayat (2).

[201] Pasal 31 UU Tipikor.

8) Undang-Undang No. 36 Tahun 1999 (UU Telekomunikasi)

Sejak tahun 1980 Indonesia telah aktif membuka arus investasi bagi industri telekomunikasi. Dalam hal kebijakan hukum, pada tahun 1989 Indonesia mulai mengembangkan peraturan di bidang telekomunikasi dengan mengesahkan Undang-Undang No. 3 Tahun 1989 tentang Telekomunikasi yang kemudian pada tahun 1999 Undang-Undang tersebut diganti dengan UU Telekomunikasi, yang membuka penguasaan investasi telekomunikasi tidak hanya dipegang oleh Badan Usaha Milik Negara (BUMN) saja.

Pada dasarnya, UU Telekomunikasi mengatur perlindungan hukum atas kebebasan sipil masyarakat dalam konteks berkomunikasi, termasuk mengenai privasi dan perlindungan data pribadi. Hal ini disebabkan karena Pasal 40 dan 42 ayat (1)UU Telekomunikasi yang secara tegas melarang segala bentuk penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi, serta mewajibkan penyelenggara jasa telekomunikasi untuk menjaga kerahasiaan informasi pengguna jasa telekomunikasi. Adapun pengecualian terhadap hal ini antara lain untuk kepentingan proses peradilan pidana atas permintaan tertulis Jaksa Agung dan/atau Kepala Kepolisian, serta penyidik yang berwenang.[202]

Jika terjadi praktik penyadapan yang melebihi ketentuan yang dimungkinkan tersebut, maka si pelanggar dapat dipidana paling singkat dua tahun atau paling lama sampai lima belas tahun dan/atau membayar denda paling banyak dua ratus juta rupiah (Rp200.000.000,00).[203]

9) Undang-Undang No. 39 Tahun 1999 (UU HAM)

Privasi merupakan hak yang fundamental sehingga harus dijamin secara hukum. Meskipun jaminan perlindungan HAM sudah termuat dalam UUD 1945 sebagai landasan konstitusional, tetapi harus diatur dalam peraturan yang lebih rinci ke dalaminstrumen setingkat Undang-Undang melalui UU HAM.

Dalam konteks privasi dan perlindungan, terdapat beberapa pasal terkait yaitu pasal Pasal 29 ayat (1), 31 dan 32. Secara umum Pasal 29 ayat (1) menyatakan pengakuan akan hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya. Perlindungan tersebut tidak hanya dalam konteks hubungan langsung, melainkan atas informasi atau data pribadi. Sedangkan, Pasal 31 disebutkan bahwa tempat kediaman seseorang "tidak boleh diganggu". Penjelasan terhadap pasal ini menunjukkan bahwa konteks frasa tersebut merujuk pada kehidupan pribadi (privasi) di dalam tempat kediamannya.

Hal lain yang perlu mendapat sorotan adalah berkaitan dengan Pasal 32 UU HAMyang juga mengatur bahwa kemerdekaan dan rahasia dalam hubungan komunikasi melalui sarana elektronik dijamin, kecuali atas perintah hakim atau kekuasaan yang lain yang sah sesuai dengan ketentuan perundang-undangan. Artinya, pasal ini memberikan ruang untuk dibatasinya penikmatan terhadap hak atas privasi seseorang.

Dalam konteks penegakan, UU HAM telah memberikan mandat kepada Komisi Nasional HAM (Komnas HAM) untuk melakukan fungsinya dalam melakukan pengkajian, penelitian,

[202] Lihat pula mekanisme proses ini dalam Pasal 87-89 Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi.

[203] Pasal 56-57 UU Telekomunikasi.

penyuluhan, pemantauan, dan mediasi tantang HAM,[204] termasuk isu hak atas privasi dan kaitannya dengan perlindungan data pribadi.

10) Undang-Undang No. 30 Tahun 2002 (UU KPK)

Dalam upaya pemberantasan korupsi yang komprehensif, khususnya dalam melakukan tugas penyelidikan, penyidikan dan penuntutan, UU KPK memberikan beberapa kewenangan kepada KPK untuk melakukan sejumlah tindakan yang dapat mengintervensi hak atas privasi seseorang. Hal tersebut tertulis dalam Pasal 12 UU KPK, khususnya huruf (a), (c) dan (f), yang menyebutkan bahwa KPK memiliki kewenangan untuk melakukan penyadapan dan merekam pembicaraan, meminta keterangan tentang keuangan tersangka atau terdakwa dan meminta data kekayaan serta perpajakan kepada bank atau lembaga keuangan serta instansi yang terkait.

Pada dasarnya, UU KPK secara tidak langsung membatasi penyidik dan penyelidik dalam mengakses data pribadi tersangka maupun terdakwa, yaitu hanya dapat dilakukan atas data yang berkaitan dengan tindak korupsi seperti harta kekayaan dan perpajakan. Hanya saja dalam UU KPK tidak memberikan pengaturan lebih lanjut mengenai pengelolaan data yang telah didapat oleh KPK khususnya terkait tindakan penyadapan. Bahkan berdasarkan Pasal 47, memungkinkan penyidik KPK dapat melakukan penyitaan tanpa izin ketua Pengadilan Negeri jika sudah memiliki bukti permulaan yang cukup.

Salah satu contoh dengan ketiadaan aturan mengenai durabilitas kewenangan melakukan penyadapan. UU Tipikor hanya menguraikan bahwa perolehan alat bukti dengan cara penyadapan dimungkinkan apabila ada dugaan berdasarkan laporan telah dan/atau akan terjadi tindak pidana korupsi,[205] dan status keabsahannya pun ditentukan oleh hakim,[206] yang terdiri atas hakim karier dan *ad hoc*.

11) Undang-Undang No. 15 Tahun 2003 (UU Anti-Terorisme)

Sebagai salah satu wujud komitmen nasional dan internasional dalam pemberantasan terorisme, Indonesia membentuk UU Terorisme yang sebelumnya merupakan Peraturan Pemerintah No. 1 Tahun 2002. Dalam regulasi ini diatur sejumlah ketentuan penegak hukum dengan kewenangan khusus untuk melakukan pemberantasan terorisme. Kewenangan tersebut adalah penyadapan dan akses data pribadi warga yang diduga terlibat dalam kejahatan terorisme.

Pasal 29 memberikan kewenangan bagi para penyidik, penuntut umum, atau kewenangan hakim untuk memerintahkan bank dan lembaga jasa keuangan. Dalam melaksanakan kewenangan tersebut, ayat (2) mengharuskan penyidik untuk membuat surat perintah yang menuliskan jelas mengenai identitas penyidik, penuntut umum atau hakim, identitas pihak yang dilaporkan oleh bank, alasan pemblokiran, tindak pidana yang disangkakan atau didakwakan, serta tempat harta kekayaan berada.

---

[204] Pasal 76 ayat (1) dan 89 UU HAM.
[205] Lihat penjelasan Pasal 28 ayat (1) UU Tipikor.
[206] *Id.*, Pasal 28 ayat (2).

Demikian pula Pasal 30 mengizinkan penyidik untuk melakukan pemeriksaan terhadap harta kekayaan pihak yang diduga atau diketahui melakukan tindak pidana terorisme. Ayat (2) Pasal yang sama menegaskan bahwa ketentuan undang-undang yang mengatur tentang kerahasiaan bank dan kerahasiaan transaksi keuangan dapat dikecualikan dengan Pasal ini. Adapun mekanisme yang harus dilakukan untuk menjalankan kewenangan tersebut diatur dalam (3) yang mewajibkan surat permintaan pemeriksaan tersebut berisikan nama atau jabatan penyidik, identitas pihak yang diduga melakukan kejahatan, pidana yang disangkakan, dan tempat harta kekayaan berada.

Dalam Pasal 31 juga disebutkan bahwa apabila sudah memiliki bukti permulaan yang cukup, penyidik berhak mengakses data pribadi seperti surat dan melakukan penyadapan pembicaraan melalui telepon atau alat komunikasi lainnya. Tindakan penyadapan hanya dilakukan atas perintah Ketua Pengadilan Negeri dalam jangka waktu 1 tahun. Pihak yang bertanggungjawab atas kewenangan penyidik tersebut adalah atasan penyidik sebagaimana diatur dalam Pasal 31 ayat (3). Meskipun tidak mengatur jelas pengakuan terhadap hak privasi, Pasal 32 mengatur mengenai kewajiban merahasiakan data pribadi terkait saksi dan pelapor. Dalam ayat (2) disebutkan bahwa dalam proses persidangan, saksi dan orang lain yang besangkutan dilarang menyebutkan identitas pelapor. Hal tersebut ditujukan untuk memberikan perlindungan bagi serta keamanan pelapor.

12) Undang-Undang No. 18 Tahun 2003 (UU Advokat)

Salah satu kewajiban seorang advokat dalam menjalankan profesinya ialah untuk menjaga rahasia kliennnya. Hal ini sebagaimana ditegaskan di dalam UU Advokat yang menyebutkan bahwa seorang advokat wajib merahasiakan segala sesuatu yang diketahui atau diperoleh dari kliennya karena hubungan profesinya, kecuali ditentukan lain oleh undang-undang.[207] Kerahasian tersebut termasuk di dalamnya perlindungan atas berkas dan dokumennya terhadap penyitaan atau pemeriksaan dan perlindungan terhadap penyadapan atas komunikasi elektronik advokat. Dari ketentuan tersebut tersurat bahwa rahasia advokat dan kliennya hanya bisa dibuka dengan menggunakan dasar undang-undang.

Namun demikian, dalam perkembangannya kemudian muncul polemik salah satunya setelah keluarnya Peraturan Pemerintah No. 43 Tahun 2015 tentang Pihak Pelapor dalam Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Pasal 3 peraturan pemerintahan ini mewajibkan para advokat untuk melaporkan kepada Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) jika ada dugaan tindak pidana pencucian uang dari pengguna jasanya. Sementara yang dimaksud dengan pengguna jasa advokat adalah klien, yang kerahasiaan diantara mereka dilindungi oleh UU Advokat.

13) Undang-Undang No. 29 Tahun 2004 (UU Praktik Kedokteran)

Secara umum UU Praktik Kedokteran mengatur perihal standar praktik dokter, khususnya standar layanan kepada pasien, prosedur administratif yang harus ditempuh untuk berpraktik, hak dan kewajiban seorang dokter, sampai dengan pengawasan dan sanksi bagi para dokter. Pada prinsipnya setiap kinerja kedokteran mengakui adanya privasi warga terkait rekam medis pasien yang dikelolanya. Dalam Pasal 47 ayat (2) disebutkan kewajiban dokter untuk menjaga

[207] Pasal 19 UU Advokat.

kerahasiaan rekam medis pasiennya, sebagai salah satu hak pasien yang harus dilindungi. Perihal tersebut ditegaskan kembali dalam Pasal 48 ayat (1) yang mengatur mengenai 'Rahasia Kedokteran'. Kewajiban dokter untuk merahasiakan rekam kesehatan pasien dilakukan seumur hidup bahkan setelah pasien itu meninggal dunia (Pasal 51 (c)). Isi rekam medis tersebut merupakan bagian dari hak pasien untuk diketahui secara pribadi (Pasal 52 poin e).

Kenyataannya kerahasiaan rekam kesehatan pasien dapat dikecualikan dalam kondisi tertentu sebagaimana diatur diatur dalam Pasal 48 ayat (2). Kondisi yang dimaksud dibatasi hanya untuk kepentingan kesehatan pasien, dalam rangka penegakan hukum, permintaan pasien sendiri, atau berdasarkan ketentuan undang-undang lainnya.

Berdasarkan Pasal 64, mekanisme yang menjamin perlindungan data pribadi dilakukan oleh Majelis Kehormatan Disiplin Kedokteran Indonesia. Pasal ini menegaskan penerimaan pengaduan, serta memeriksa dan memutuskan kasus pelanggaran dokter. Kasus pelanggaran tersebut tidak lain juga termasuk adanya kebocoran data pasien. Adapun mekanisme pengaduan tersebut diatur dalam Pasal 66-70. Bahkan dalam Pasal 79 (c) ditegaskan adanya ancaman pidana paling lama 1 tahun dan denda lima puluh juta rupiah (Rp50.000.000,00) yang tidak menjalankan kewajiban menjaga rahasia kesehatan pasien.

Lebih lanjut aturan teknis implementatif mengenai rahasia kedokteran diatur melalui Peraturan Menteri Kesehatan No. 36 Tahun 2012 tentang Rahasia Kedokteran. Peraturan ini mengatur secara lebih terperinci mengenai cakupan rahasia kedokteran, penyimpanan, pembukaan, hingga pengawasannya. Menurut peraturan ini rahasia kedokteran bisa dibuka hanya untuk kepentingan kesehatan pasien, memenuhi permintaan aparatur penegak hukum dalam rangka penegakan hukum, permintaan pasien sendiri atau berdasarkan ketentuan peraturan perundang-undangan.

14) Undang-Undang No. 24 Tahun 2013 (UU Adminduk)

UU Adminduk mengatur mengenai kegiatan administrasi kependudukan sebagai rangkaian kegiatan penataan dan penertiban dalam penerbitan dokumen dan data kependudukan, termasuk data pribadi penduduk,[208] melaluiSistem Informasi Administrasi Kependudukan (SIAK). Berdasarkan Pasal 85 UU Adminduk, negara memiliki kewajiban untuk menyimpan dan memberikan perlindungan atas data pribadi penduduk tersebut. Hal tersebut juga tercantum dalam Pasal 79 yang mewajibkan negara untuk memberikan perlindungan dan menunjuk menteri sebagai penanggung jawab hak akses data pribadi warga. Demikian pula dalam UU Adminduk terbaru dalam Pasal 1 poin 22 mengakui data pribadi sebagai data perseorangan yang harus disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiaannya.

Keberadaan pasal-pasal diatas menyebabkan hak akses petugas Penyelenggara dan Instansi Pelaksana pengumpul data pribadi penduduk berkewajiban untuk menjaga informasi dan kerahasiaan data tersebut, yang pengaturannya secara lebih rinci dimuat dalam Peraturan Presiden No. 67 Tahun 2011 tentang Kartu Tanda Penduduk Berbasis Nomor Induk

[208] Pasal 84 ayat (1) UU Adminduk menegaskan sejumlah data yang masuk dalam kategori data pribadi penduduk, yaitu (a) nomor Kartu Keluarga (KK), (b) Nomor Induk Kependudukan (NIK), (c) tanggal, bulan atau tahun lahir, (d) keterangan tentang kecacatan fisik dan/atau mental, (e) NIK ibu kandung, (f) NIK ayah, dan (g) beberapa isi catatan peristiwa penting.

Kependudukan Secara Nasional. Akan tetapi, peraturan ini masih belum mengakomodasi perlindungan data pribadi penduduk (penyimpanan dan penggunaannya), kaitannya dengan pasca-pemindaian dan perekaman data yang menyangkut sidik jari dan retina mata penduduk.

Sebagai tambahan untuk konteks pengawasan terhadap data pribadi penduduk diatur lebih lanjut dalam Peraturan Pemerintah No. 37 Tahun 2007 tentang Pelaksanaan UU Adminduk, khususnya pada Pasal 5 ayat (1) yang menegaskan bahwa Menteri Dalam Negeri RI (Mendagri) memiliki kewenangan untuk mengawasi pelaksanaan SIAK.

Sedangkan dalam hal mekanisme pemulihan terjadinya pelanggaran, UU Adminduk mengakui hak penduduk untuk memperoleh ganti rugi serta pemulihan akibat penyalahgunaan data pribadi oleh instansi pelaksana[209] Bahkan dalam Pasal 95 menegaskan adanya ancaman pidana maksimal 2 tahun dan denda dua puluh lima juta rupiah (Rp25.000.000,00) terhadap pihak yang mengakses *database* kependudukan secara melawan hukum. Sedangkan, jika pelanggaran dilakukan oleh pejabat atau petugas instansi pelaksana, maka pidana tersebut ditambah satu per tiga dari sanksi yang telah ditetapkan.[210]

15) Undang-Undang No. 21 Tahun 2007 (UU TPPO)

Sebagai upaya pemberantasan tindak pidana perdagangan orang di Indonesia, UU TPPO memberikan sejumlah kewenangan yang mengintrusi hak privasi warga dalam kepentingan penegakan hukum. Tindakan tersebut adalah kewenangan penyadapan dan mengakses data pribadi tersangka atau pihak yang diduga kuat melakukan kejahatan tersebut. Dalam hal data penyidikan, penjelasan Pasal 29 menegaskan bahwa ruang lingkup 'data' termasuk catatan rekening bank atau keuangan, catatan pergerakan, perjanalan, atau komunikasi, serta dokumen lain. Artinya, penyidik memiliki wewenang untuk mengakses data pribadi pihak tersebut. Bahkan dalam Pasal 32 disebutkan bahwa penyidik, penuntut umun, atau hakim berwenang memerintahkan penyedia jasa keuangan untuk melakukan pemblokiran terhadap harta kekayaan pihak yang disangka atau didakwa melakukan tindak pidana perdagangan orang.

Sedangkan perihal penyadapan, Pasal 31 UU TPPO menyebutkan bahwa penyidik dapat melakukan penyadapan melalui telepon atau alat komunikasi lain harus didasarkan pada bukti permulaan yang cukup. Selain itu dalam ayat (2) disebutkan, prosedur penyadapan harus melalui izin tertulis ketua Pengadilan dalam jangka waktu paling lama 1 tahun.

Selain kewenangan penyadapan dan intrusi data pribadi, UU TPPO melalui Pasal 33 menegaskan adanya perlindungan data pribadi pihak saksi atau terlapor. Pelapor berhak meminta kepada penyidik agara menjaga kerahasiaan identitas pelapor seperti nama dan alamat. Sehingga menjadi kewajiban bagi penyidik untuk merahasiakan identitas pelapor dalam proses penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan.

[209] Pasal 2 huruf (f) UU Adminduk.
[210] *Id.*, Pasal 98.

16) Undang-Undang No. 11 Tahun 2008 (UU ITE)

Perkembangan pemanfaatan teknologi internet yang semakin meningkat, menyebabkan terbukanya akses media informasi yang luas. Hal ini berpengaruh pula pada kemampuan akses mengenai data yang bersifat informasi publik maupun informasi pribadi. Dalam UU ITE disebutkan secara implisit mengenai perlindungan terhadap keberadaaan suatu data atau informasi elektronik baik yang bersifat umum maupun pribadi.

Adapun pengaturan tersebut terkait mengenai perlindungan dari tindakan penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses intervensi ilegal. Salah satunya dalam Pasal 26 UU ITE yang mensyaratkan bahwa penggunaan setiap data pribadi dalam sebuah media elektronik harus mendapatkan persetujuan pemilik data yang bersangkutan. Sehingga, pelanggaran atas tindakan tersebut dapat diguguat atas kerugian yang ditimbulkan. Dalam penjelasan pasalnya dikatakan bahwa Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi *(privacy rights)*. Lebih jauh menurut ketentuan ini yang dimaksud hak pribadi di dalamnya termasuk: (i) hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan; (ii) hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai; dan (iii) hak untuk mengawasi akses informasi kehidupan pribadi dan data seseorang.

Selain itu dalam ketentuan Pasal 43 ayat (2) juga disebutkan esensi perlindungan data pribadi warga negara, meski dalam proses pidana sekalipun. Dikatakan dalam ketentuan tersebut, bahwa dalam setiap penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik haruslah dilakukan dengan memperhatikan perlindungan terhadap privasi,kerahasiaan, kelancaran layanan publik, integritas data,atau keutuhan data sesuai dengan ketentuan peraturan perundang-undangan. Selanjutnya, sebagaimana juga diatur di dalam KUHAP, pada ketentuan Pasal 43 ayat (3) UU ITE ditegaskan bahwa setiap penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua Pengadilan Negeri setempat.

Terkait bentuk perlindungannya, UU ITE membuka jalan untuk mengajukan gugatan atas kerugian pelanggaran data pribadi.[211] Hal ini ditegaskan kembali dalam Pasal 38 yang menyebutkan bahwa setiap pihak yang merasa dirugikan dari penyelenggaraan sistem elektronik teknologi informasi dapat mengajukan gugatan. Terkait praktik penyadapan yang diatur dalam Pasal 31, pelanggarannya diatur dalam pasal 47. Dalam pasal tersebut ditegaskan ancaman pidana paling lama sepuluh tahun dan denda paling banyak delapan ratus juta rupiah (Rp800.000.000,00).

Sebagai turunan dari UU ITE, kemudian dibentuk PP PSTE yang menyebutkan secara jelas mengenai perlindungan data pribadi. Terminologi data pribadi menurut Peraturan Pemerintah ini diartikan sebagai data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Salah satu betuk data yang paling dilindungi adalah berbentuk informasi elektronik yang menurut Pasal 1 ayat (6) PP PSTEdijelaskan sebagai satu atau sekumpulan data elektronik termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau

[211] Pasal 26 ayat (2) UU ITE.

perforasi. Informasi elektronik ini dapat ditemukan dalam sistem elektronik atau berupa sebuah dokumen elektronik. Pasal 15 PP PSTE ditegaskan pula penyelenggara sistem elektronik wajib menjaga kerahasiaan, keutuhan dan ketersediaan data pribadi yang dikelola.

Pelanggaran terhadap upaya perlindungan data pribadi ini, penyelenggara sistem elektronik maupun agen akan diberikan sanksi administratif sebagaimana terdapat dalam Pasal 84 PP PSTE. Sanksi administratif tersebut dapat berupa teguran tertulis, denda administratif, penghentian sementara, serta dikeluarkan dari daftar penyelenggara sistem elektronik, agen elektronik, penyelenggara sertifikasi elektronik atau lembaga sertifikasi keandalan.

Sedangkan untuk aspek pengawasan, Pasal 33 ayat (1) PP PSTE memberikan mandat kepada Menteri Komunikasi dan Informatika RI (Menkominfo) sebagai lembaga yang berwenang untuk mengawasi setiap penyelenggaraan sistem elektronik, termasuk kaitannya dengan intrusi terhadap data pribadi dalam sistem elektronik.

17) Undang-Undang No. 14 Tahun 2008 (UU KIP)

Dalam pengelolaan demokrasi dalam konteks pemerintahan yang baik, Indonesia turut mengeluarkan peraturan perundangan terkait pengelolaan informasi khususnya keterbukaan informasi. Berdasarkan Pasal 1 ayat (1) UU KIP diatur mengenai informasi yang diartikan sebagai keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung niai, makna, dan pesan, baik data, fakta maupun penjelasan yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun non-elektronik. Sedangkan terminologi informasi publik itu sendiri diartikan sebagai informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh stau Badan Publik yang berkaitan dengan penyelenggaraan negara dan/atau penyelenggara dan penyelenggaraan Badan Publik lainnya yang berkaitan dengan kepentingan publik. Dari definisi informasi publik tersebut, terlihat bahwa badan publik sebagaimana yang diatur dalam undang-undang melakukan pengumpulan data dan informasi yang berkaitan dengan penyelenggaraannya.

Meskipun secara umum undang-undang ini membantu akses terhadap data dan informasi yang dihimpun oleh badan publik, tetapi terdapat pengecualian terhadap informasi terkait data pribadi. Dalam Pasal 6 ayat (3) huruf (c) UU KIP yang menegaskan kepada badan publik untuk tidak memberikan informasi publik yang berkaitan dengan hak-hak pribadi. Hal tersebut juga tertulis dalam butir Pasal 17 huruf (g)-(h) yang menyebutkan bahwa akta otentik yang bersifat pribadi dan kemauan terakhir atau wasiat seseorang serta informasi yang berkaitan dengan rahasia pribadi dinyatakan sebagai informasi yang dikecualikan. Adapun informasi yang dapat mengungkap rahasia pribadi adalah berkaitan dengan riwayat dan kondisi anggota keluarga, pengobatan kesehatan fisik dan psikis seseorang, kondisi keuangan, pendapatan dan rekening bank seseorang, serta riwayat pendidikan formal dan satuan pendidikan non-formal.[212]

Pengaturan tersebut menunjukkan adanya kewajiban untuk memberikan perlindungan terhadap informasi badan publik yang berkaitan dengan hak-hak pribadi. Dengan kata lain UU

[212] Lihat pula Bab IV Peraturan Komisi Informasi Nomor 1 Tahun 2010 tentang Standar Layanan Informasi Publik (PerKIP No. 1 Tahun 2010).

KIP memberikan kewenangan untuk melakukan *self-control* pada setiap badan publik dalam hal perlindungan data pribadi untuk tidak disebarkan secara publik. Kewenangan kontrol internal tersebut merupakan bagian dari uji konsekuensi yang wajib dilakukan badan publik untuk membuat analisis dampak terbukanya informasi tersebut.[213] Hal ini juga akan berkaitan erat dengan kewenangan Komisi Informasi (KI) untuk mengawasi perlindungan terhadap informasi yang bersifat pribadi tersebut melalui evaluasi terhadap laporan layanan informasi publik yang disampaikan oleh badan publik yang bersangkutan.[214]

Meskipun demikian, terkait kewenangannya yang diatur dalam Pasal 23 dan 26 UU KIP memungkinkan KI untuk mengkualifikasi sebuah informasi sebagai data pribadi. Misalnya dalam hal penyelesaian sengketa, tidak jarang menetapkan putusan KI memuat sejumlah informasi tidak dapat dibuka secara publik dengan alasan terkait Pasal 17.

18) Undang-Undang No. 21 Tahun 2008 (UU Perbankan Syariah)

Sebagai instrumen yang lahir sebagai dampak dari maraknya praktik perbankan syariah, UU Perbankan Syariah dibentuk dengan harapan agar kehidupan perbankan di Indonesia tidak hanya melulu terfokuskan pada kegiatan perbankan konvensional, tetapi juga memberikan ruang gerak bagi kegiatan perbankan syariah yang pada saat itu belum memiliki kerangka regulasi yang spesifik mengatur hal tersebut.

Secara materiil, UU Perbankan Syariah memiliki kesamaan muatan dengan UU Perbankan, termasuk hal-hal yang berkaitan dengan perlindungan data pribadi. Pasal 41 UU Perbankan Syariah mengatur mengenai mandat bank untuk menjaga kerahasiaan data nasabah penyimpan dan simpanannya, kecuali untuk hal-hal tertentu yang dimungkinkan oleh undang-undang. Pengecualian tersebut tidak lain ditujukan untuk kepentingan penyidikan perpajakan yang memungkinkan dibukanya keadaan keuangan Nasabah sebagaimana diatur dalam Pasal 42 (1) hingga Pasal 49.

Dalam hal pengecualian tersebut, Pasal 42 ayat (1) mengatur mekanisme yang harus dilakukan pihak aparat penegak hukum seperti menyebutkan nama pejabat pajak, nama nasabah wajib pajaks sreta penjelasan kasus yang berkaitan. Pasal 50 UU Perbankan Syariah telah memberikan kewenangan kepada BI untuk melakukan pengawasan terhadap semua aktivitas bank syariah, termasuk yang bersinggungan dengan penegakan prinsip kerahasiaan bank.

Instrumen penjatuhan sanksi baik secara administratif dan pidana sebagai bentuk menjaga perlindungan privasi nasabah.[215] Dalam Pasal 60 dijelaskan bahwa setiap orang yang meminta pihak bank untuk memberikan keterangan tanpa melalui prosedur yang berlaku diancam pidana penjara paling singkat 2 tahun dan paling lama 4 tahun serta denda sebesar sepuluh miliar (Rp10.000.000.000,00) hingga dua ratus miliar rupiah (Rp200.000.000.000,00). Begitu pula dalam pengaturan internal, tindakan yang pejabat dan pegawai bank yang tidak memenuhi kewajiban perlindungan data pribadi nasabah diancam pidana penjara paling singkat 2 tahun dan denda dengan kisaran empat hingga lima belas miliar rupiah.

---

[213] Pasal 19 UU KIP.
[214] *Id.*, Pasal 36-37.
[215] Pasal 57 UU Perbankan Syariah.

Namun, pasca berdirinya OJK, kewenangan BI tersebut secara otomatis dilimpahkan kepada OJK, khususnya dikelola oleh Departemen Perbankan Syariah (DPBS). Pada praktiknya, DPBS dalam menjalankan kewenangan pemantauan ini pun sering kali bekerjasama dengan Dewan Syariah Nasional Majelis Ulama Indonesia (DSN MUI).[216]

19) Undang-Undang No. 35 Tahun 2009 (UU Narkotika)

Dalam upaya memberantas tindak pidana narkotika, undang-undang ini memberikan kewenangan kepada Badan Narkotika Nasional (BNN) untuk melakukan serangkaian kegiatan yang mengintervensi hak privasi warga. Kegiatan tersebut adalah terkait kewenangan penyadapan dan akses terhadap data kekayaan dan perpajakan terkait penyalahgunaan, peredaran gelap, dan prekursor narkotika yang dilakukan oleh tersangka. Kewenangan tersebut berdasarkan Pasal 75 huruf (i) UU Narkotika. Dalam pelaksanaannya, mekanisme penyadapan untuk tindak pidana penyalahgunaan narkotika diatur dalam Pasal 77. Pasal tersebut menyebutkan penyadapan dapat dilakukan setelah mendapatkan bukti permulaan yang cukup dengan jangka waktu 3 bulan terhitung dari surat penyadapan diterima penyidik. Surat penyadapan tersebut diperoleh dari izin ketua Pengadilan sebagaimana disebutkan dalam dalam ayat (2). Berdasarkan ayat (3) tindakan penyadapan dapat diperpanjang satu (1) kali untuk jangka waktu yang sama, tanpa mengatur batasan berapa kali dapat mengajukan perpanjangan.

Meskipun demikian, dalam Pasal 78 memungkinkan Penyidik dapat melakukan penyadapan ntanpa izin tertulis dari Ketua Pengadilan Negeri. Hanya saja dalam ayat (2) disebutkan bahwa dalam waktu satu kali dua puluh empat jam Penyidik wajib meminta izin tertulis kepada ketua Pengadilan. Selain penyadapan, tindakan UU Narkotika melalui Pasal 80 juga mengizinkan penyidik untuk mengakses data pribadi terkait kewenangan penyidik untuk meminta data kekayaan dan perpajakan tersangka.

20) Undang-Undang No. 36 Tahun 2009 (UU Kesehatan)

Berdasarkan ketentuan Pasal 52 ayat (2) UU Kesehatan, tenaga kesehatan dalam melakukan tugasnya berkewajiban untuk mematuhi standar profesi dan menghormati hak pasien. Salah satu bentuk penghormatan tersebut adalah terkait dengan hak atas informasikesehatan pribadinya.[217] Hal ini tertulis dalam Pasal 57 ayat (1) undang-undang ini yang berbunyi hak setiap orang atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan. Namun, hak ini dapat dikecualikan jika terkait dengan penegakan hukum dan kepentingan lain-lain sebagaimana diatur dalam Pasal 57 ayat (2).

Mekanisme perlindungan data kesehatan pasien dapat diartikan sebagai salah satu kewajiban dalam penyelengagran pelayanan kesehatan sebagaimana diatur dalam Pasal 54. Pasal tesebut menjelaskan bahwa pelaksanaan tersebut harus dilaksanakan secara aman, bermutum bertanggung jawab, merata dan tidak diskriminatif. Bahkan, menegaskan tugas Pemerintah dan Pemerintah Daerah untuk setiap penyelenggaraan kesehatan, yang dapat diartikan termasuk kewenangan menjaga kerahasiaan data kesehatan pasien, sedangkan dalam Pasal 55

[216] Informasi lebih lanjut terkait DSN MUI dapat dilihat pada <http://www.dsnmui.or.id/>.
[217] Pasal 8 UU Kesehatan.

disebutkan bahwa pemerintah wajib menetapkan standar mutu pelayanan. Adapun standar mutu pelayanan ini juga dapat termasuk perlindungan data privasi kesehatan pasien.

Meskipun demikian UU Kesehatan ini tidak mengatur penuh mengenai mekanisme pemulihan bagi pemegang hak (dalam hal ini pasien) atas pelanggaran terhadap perlindungan data pribadi pasien tersebut. Undang-undang ini tidak memuat pengaturan sanksi atau hukuman, baik secara administratif ataupun pidana, bagi pelanggaran privasi atas riwayat kesehatan pasien tersebut.[218] Ketentuan yang ada hanyalah sebatas kepada pen-delegasian kewenangan Menteri Kesehatan RI (Menkes) untuk mengawasi penyelenggaraan kegiatan di bidang kesehatan, termasuk penggunaan riwayat kesehatan pasien.[219] Sebagai kelanjutan dari delegasi pengaturan tersebut, Menkes setidaknya telah mengeluarkan tiga peraturan terkait dengan perlindungan data pribadi pasien, yakni: (i) Peraturan Menteri Kesehatan No. 269/Menkes/Per/III/2008 tentang Rekam Medis (Permenkes Rekam Medis); (ii) Peraturan Menteri Kesehatan No. 36 Tahun 2012 tentang Rahasia Kedokteran; dan (iii) Peraturan Menteri Kesehatan No. 55 Tahun 2013 tentang Penyelenggaraan Pekerjaan Rekam Medis.

Ketiga peraturan tersebut mengatur mengenai cakupan rekam medis (data kesehatan pasien), penyimpanan, pembukaan, pengawasan, kualifikasi, serta hak dan kewajiban petugas kesehatan yang melakukan perekaman medis.

21) Undang-Undang No. 43 Tahun 2009 (UU Kearsipan)

Dalam proses kegiatan administrasi negara terdapat penyelenggaraan sistem kearsipan oleh pemerintah. Sistem kearsipan tidak jarang mencakup data/informasi pribadi seseorang, misalnya data kependudukan, serta data tenaga pengajar dan pelajar dalam perguruan tinggi.[220] Pada dasarnya, sistem kearsipan diatur dalam UU Kearsipan yang mengatur aspek publik pengarsipan penyelenggaraan administrasi negara. Dalam Pasal 3 huruf (f) Undang-Undang tersebut dinyatakan bahwa salah satu tujuan kearsipan ialah untuk menjamin keselamatan dan keamanan arsip sebagai bukti pertanggung-jawaban dalam kehidupan bermasyarakat, berbangsa, dan bernegara. Sedangkan mengenai jaminan terhadap keamanan data tersebut, UU Kearsipan telah mencantumkan ancaman sanksi administratif dan sanksi pidana terhadap siapa saja yang menyalahi penggunaan arsip negara berdasarkan ketentuan yang telah disediakan dalam undang-undang ini.[221]

Dalam menjamin efektivitas pengimplementasian UU Kearsipan ini, Peraturan Kepala Arsip Nasional RI (Perka ANRI) Nomor 38 Tahun 2015 tentang Pedoman Pengawasan Kearsipan telah mengamanahkan Tim Pengawas Kearsipan, yang terdiri dari Tim Pengawas Kearsipan Eksternal[222] dan Internal[223] untuk bahu-membahu mensupervisi pelaksanaan penyelenggaraan kearsipan dan penegakan peraturan perundang-undangan di bidang kearsipan.

[218] Naskah Akademik RUU PDP, *Op.Cit.*, hal.68.
[219] Pasal 182-188 UU Kesehatan.
[220] Pasal 5 ayat (1) UU Kearsipan
[221] Pasal 78-88 UU Kearsipan tentang sanksi administratif dan sanksi pidana
[222] Perka ANRI No. 38 Tahun 2015, Pasal 4 ayat (1).
[223] *Id.*, Pasal 7 ayat (1).

22) Undang-Undang No. 44 Tahun 2009 (UU Rumah Sakit)

Sama halnya dengan UU Kesehatan, perlindungan data pasien terhadap pelaksanaan kegiatan rekam medis yang dilakukan oleh rumah sakit diakui keberadaannya dalam Pasal 29 ayat (1) huruf (h), (l), dan (m) UU Rumah Sakit. Pengakuan privasi tersebut merupakan bagian dari hak pasien sebagaimana tertera dalam Pasal 32 huruf (i). Hal ini kembali ditegaskan dalam Pasal 38 ayat (1) yang mewajibkan rumah sakit untuk menyimpan rahasia kedokteran. Serta Pasal 44 yang memiliki wewenang untuk mengungkapkan segala informasi kepada publik yang berkaitan dengan rahasia kedokteran. Meskipun demikian perlindungan hak privasi tersebut dapat dibatasi. Dalam pasal 38 poin (2) dijelaskan bahwa dalam rangka penegakan hukum, atas persetujuan pasien sendiri kerahasian data kesehatan pasien dapat dibocorkan.

Mengenai mekanisme perlindungannya, Pasal 54-55 undang-undang ini menyebutkan tugas Pemerintah dan Pemerintah Daerah dalam melakukan pembinaan dan pengawasan terhadap Rumah Sakit dengan melibatkan organisasi profesi dan asosiai perumahsakitan. Adapun salah satu tugas tersebut juga menyangkut kewajiban melindungi kerahasiaan data kesehatan pasien yang merupakan tanggung jawab profesi tenaga kesehatan, termasuk rumah sakit.

Sehubungan dengan hal itu, sebagai upaya untuk menjamin pelaksanaan kegiatan rekam medis tersebut, Pasal 16 ayat (1) Permenkes Rekam Medis memberikan kewenangan kepada Kepala Dinas Kesehatan (Ka. Dinkes) Provinsi, Ka. Dinkes Kabupaten/Kota dan organisasi profesi terkait untuk mengawasi praktik rekam medis yang dilakukan oleh rumah sakit. Selain itu secara khusus Kementerian Kesehatan juga telah mengeluarkan Peraturan Menteri Kesehatan No. 1171/Menkes/Per/VI/2011 tentang Sistem Informasi Rumah Sakit. Ketentuan mengenai data pribadi terutama terkait erat dengan penyelenggaraan data mengenai kompilasi penyakit/morbiditas pasien.

23) Undang-Undang No. 8 Tahun 2010 (UU TPPU)

Berdasarkan ketentuan dalam UU TPPU,PPATK memiliki wewenang untuk melakukan tindakan untuk mengintrusi hak privasi warga negara, dalam rangka mencegah dan memberantas tindak pidana pencucian uang. Undang-undang ini menegaskan bahwa dalam melaksanakan tugasnya, PPATK berwenang untuk meminta dan mendapatkan data dari instansi pemerintah dan/atau lembaga swasta yang memiliki kewenangan mengelola data termasuk dari instansi pemerintah atau lembaga swasta yang menerima laporan dari profesi tertentu.[224] Lebih lanjut, Pasal 41 ayat (2) UU TPPU disebutkan bahwa data atau informasi yang dapat diakses PPATK adalah data yang berkaitan dengan transaksi keuangan dari hasil tindak pidana. Kewenangan tersebut mengecualikan kewajiban menjaga kerahasiaan yang harusnya dijalankan sejumlah lembaga yang didefinisikan sebagai Pihak Pelapor.[225]

Hal serupa juga disebutkan dalam Pasal 45, yang mengatur mengenai kinerja PPATK mengecualikan prinsip hak privasi dan kode etik yang mengatur kerahasiaan. Demikian pula dalam Pasal 72 ayat (2) dijelaskan bahwa dalam meminta keterangan terkait perkara pencucian uang (*money laundering*), ketentuan undang-undang yang mengatur rahasia bank dan

[224] Pasal 40, 41 ayat (1) huruf (a) UU TPPU.
[225] *Id.*, Pasal 28.

transaksi keuangan lainnya tidak berlaku bagi tim penyidik, penuntut umum dan hakim yang sedang menanganinya.

Dalam menjalankan tugas tersebut, pegawai PPATK dan pihak yang mendapatkan wewenang untuk memperoleh dokumen memiliki kewajiban untuk merahasiakannya, kecuali untuk memenuhi kewajiban undang-undang ini.[226]Dalam Pasal 54 ayat (2) juga disebutkan dalam salah satu klausul janji atau sumpah yang diucapkan Kepala dan Wakil PPATK yaitu harus merahasiakan hal-hal yang menurut peraturan perundang-undangan wajib dirahasiakan. Kewajiban menjaga privasi juga dilakukan dlam rangka melindungi Pihak Pelapor dan saksi.[227]

Dalam hal pengelolaan data, Pasal 42 UU TPPU hanya menjelaskan kewenangan PPATK dalam menyelenggarakan sistem informasi, tanpa secara khusus memberikan pengaturan mengenai perlindungan privasi/data pribadi pihak terkait. Namun demikian, merujuk pada ketentuan Pasal 40 UU TPPU, PPATK juga diharuskan untuk melakukan pengelolaan data dan informasi yang diperolehnya, sebagai bagian dari fungsinya tersebut.

Mengenai otoritas yang berwenang untuk memberikan izin kepada PPATK dalam mengakses data tersebut, Penjelasan Pasal 41 ayat (2) disebutkan bahwa penyampaian data dan informasi oleh instansi pemerintah dan/atau lembaga swasta tidak memerlukan izin siapapun. Sedangkan untuk pengaturan lebih lanjut mengenai tata cara penyampaian data dan informasi disebutkan sesuai harus dengan Peraturan Pemerintah yang hingga saat ini belum terbentuk.

Meskipun demikian, mekanisme perlindungan data pribadi diberikan bagi saksi, yang merasa dirugikan terkait kegagalan pejabat PPATK dalam merahasiakan identitasnya. Mekanisme tersebut tidak lain adalah menuntut ganti kerugian melalui pengadilan sebagaimana diatur dalam Pasal 83.

24) Undang-Undang Nomor 17 Tahun 2011 (UU Intelijen Negara)

Dalam menjalankan tugas intelijen negara, Badan Intelijen Negara (BIN) diberikan wewenang untuk melakukan penyadapan, pemeriksaan aliran dana dan penggalian informasi, sebagai diatur ketentuan Pasal 31 UU Intelijen Negara. Guna mendapatkan informasi aliran dana dan menggali informasi demi kepentingan intelijen negara, BIN dapat meminta dari penegak hukum dan lembaga terkait, dengan perintah dari Kepala BIN.[228] Pemberian wewenang ini tentunya berpotensi bagi terjadinya intrusi terhadap perlindungan data pribadi seseorang.

Sehubungan dengan hal ini, Pasal 15 ayat (1) UU Intelijen Negara membuka ruang kepada pihak yang dirugikan akibat dari pelaksanaan fungsi intelijen untuk mengajukan permohonan rehabilitasi, kompensasi, dan restitusi. Meskipun tidak dijelaskan secara detail apa yang dimaksud dengan "dirugikan akibat pelaksanaan fungsi intelijen", tetapi hal ini dapat diartikan pula termasuk di dalamnya kerugian warga negara yang merasa privasinya dilanggar akibat dari suatu aktivitas intelijen negara. Selain itu, katup perlindungan lainnya diatur di dalam Pasal 47 yang menyebutkan bahwa setiap Personel Intelijen Negara yang melakukan penyadapan di luar fungsi penyelidikan, pengamanan dan penggalangan sebagaimana

[226] *Id.*, Pasal 11 ayat (1).
[227] *Id.*, Pasal 83.
[228] Pasal 32-34 UU Intelijen Negara.

dimaksud dalam Pasal 32 UU Intelijen Negara, dipidana dengan pidana penjara paling lama lima tahun dan/atau pidana denda paling banyak lima ratus juta rupiah (Rp500.000.000,00).

25) Undang-Undang No. 18 Tahun 2011 (UU KY)

Keberadaan Komisi Yudisial (KY) memiliki tujuan untuk merujudkan kekuasaan kehakiman yang merdeka untuk menjalankan peradilan dan penegakkan hukum yang berkeadilan. Dalam rangka itulah UU KY memberikan sejumlah kewenangan kepada KY, termasuk yang membatasi hak privasi seseorang. Dalam Pasal 20 disebutkan bahwa Komisi ini dapat meminta aparat penegak hukum untuk melakukan penyadapan dan merekam pembicaraan hakim, sekiranya ada dugaan pelanggaran kode etik kehakiman. Selain itu, untuk melakukan pengawasan, KY dapat meminta keterangan atau data kepada Badan Peradilan dan/atau Hakim dan melalui Mahkamah Agung seperti yang diatur dalam Pasal 22. Data yang dimaksud tersebut adalah informasi yang berkaitan dengan proses peradilan dan dugaan pelanggaran kode etik. Meskipun demikian, tidak dijelaskan lebih lanjut jenis data yang dimaksud, termasuk data pribadi hakim atau tidak.

26) Undang-Undang No. 21 Tahun 2011 (UU OJK)

Pada perkembangannya, mekanisme pengawasan akan perlindungan data pribadi nasabah bank dalam konteks *bank secrecy*, yang sebelumnya menjadi wewenang Bank Indonesia, sebagaimana termaktub dalam UU Perbankan, UU Perbankan Syariah dan UU Bank Indonesia, sejak disahkannya UU OJK, telah dipindahtangankan fungsinya kepada OJK.[229]Hal ini mengacu pada ketentuan Pasal 5, 6 huruf (a) dan 7 UUOJK.

Ketentuan ini kemudian diperkukuh kembali melalui Peraturan OJK (POJK) Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, yang pada butir Pasal 2 huruf (d) menegaskan adanya prinsip dasar perlindungan konsumen yang harus OJK emban adalah berdasarkan pada prinsip kerahasiaan dan keamanan data/informasi konsumen. Bahkan, POJK ini memuat pula Bab khusus yang mengatur mengenai pengawasan perlindungan konsumen sektor jasa keuangan sepenuhnya berada pada kewenangan OJK.[230] Dengan kata lain, esensi perlindungan data pribadi nasabah bank menjadi hal yang disoroti pula oleh OJK ketika melaksanakan fungsi pengawasannya tersebut.

OJK bahkan secara lebih terperinci memuat daftar data dan/atau informasi pribadi konsumen yang harus dirahasiakan melalui Surat Edaran OJK (SE-OJK) Nomor 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen, berupa nama, alamat, nomor telepon, tanggal lahir dan/atau umur, dan/atau nama ibu kandung (khusus nasabah perorangan), serta susunan direksi dan komisaris termasuk dokumen identitas berupa Kartu Tanda Penduduk/paspor/izin tinggal, dan/atau susunan pemegang saham (khusus untuk nasabah korporasi).

[229] Marnia Rani, "Perlindungan Otoritas Jasa Keuangan terhadap Kerahasiaan dan Keamanan Data Pribadi Nasabah Bank", 2 *Jurnal Selat* 1, (2014) hal.171.
[230] Lihat Pasal 51-52 POJK No. 1/POJK.07/2013.

27) Undang-Undang No. 9 Tahun 2013 (UU Pendanaan Terorisme)

Pengawasan dalam bidang pendanaan dinilai menjadi salah satu upaya pencegahan yang efektif dalam memberantas tindak pidana terorisme. Hal ini disebabkan karena unsurpendanaan terorisme merupakan salah satu faktor utama dalam setiap aksi terorisme, sehingga upaya penanggulangan terorisme harus diikuti dengan upaya pencegahan dan pemberantasan terhadap pendanaan terorisme. Dalam rangka itulah, UU Pendanaan Terorisme memberikan kewenangan kepada sejumlah institusi pemerintah dan penegak hukum untuk melakukan pengamatan serta mengakses data pribadi warga negara yang terindikasi akan melakukan tindak terorisme. Pemberian wewenang tersebut tentunya akan berpotensi membuka celah terjadinya pelanggaran terhadap hak atas privasi warga negara, khususnya terkait dengan data-data pribadinya, terutama data perbankan.

Sebagai katup pengaman untuk menjaga kerahasiaan atas data-data tersebut, ketentuan dalam UU Pendanaan Terorisme menyebutkan bahwa pejabat atau pegawai PPATK, penyidik, penuntut umum, hakim atau setiap orang yang memperoleh dokumen atau keterangan berkaitan dengan transaksi keuangan mencurigakan, terkait pendanaan terorisme, memiliki kewajiban untuk merahasiakan dokumen itu.[231] Bahkan,undang-undang ini juga menyatakan apabila pihak tersebut membocorkan rahasia dokumen terkait pendanaan tersebut, maka yang bersangkutan dapat dipidana paling lama empat tahun.[232] Keberadaan pasal ini menunjukkan adanya perlindungan data pribadi terkait transaksi keuangan yang dicurigai terlibat pendanaan terorisme.

28) Undang-Undang No. 7 Tahun 2014 (UU Perdagangan)

Ketentuan UU Perdagangan memang tidak secara khusus mengatur mengenai perlindungan data pribadi konsumen. Namun demikian, di dalam undang-undang ini ditegaskan bahwa dalam perdagangan yang menggunakan sistem elektronik (*e-commerce*), setiap pelaku perdagangan harus sepenuhnya mengacu pada ketentuan yang berlaku dalam UU ITE.[233] Artinya, ketentuan mengenai perlindungan data pribadi juga mengikat seutuhnya dalam setiap perdagangan yang memanfaatkan sistem elektronik.

Sedangkan mengenai mekanisme perlindungannya, dalam Pasal 65 ayat (5) dijelaskan bahwa sengketa terkait transaksi dagang dengan sistem elektronik diselesaikan melalui pengadilan dan mekanisme penyelesaian sengketa lainnya. Undang-undang ini juga mengatur mengenai sanksi administrasi bagi pelaku usaha yang tidak memenuhi ketentuan penyediaan data/informasi secara lengkap dan benar.[234] Dalam hal ini tidak dijelaskan secara jelas apakah perihal perlindungan data pribadi juga dimaksudkan dalam poin ini atau tidak.

Oleh karenanya, pembentukan peraturan pemerintah mengenai perdagangan melalui sistem elektronik yang dimandatkan oleh Pasal 66 UU Perdagangan, semestinya juga mengatur mengenai perlindungan data pribadi konsumen, dengan merujuk pada peraturan perundang-undangan yang ada, terutama UU ITE dan UU Perlindungan Konsumen.

---

[231] Pasal 9 ayat (1) UU Pendanaan Terorisme.
[232] *Id.*, Pasal 9 ayat (2).
[233] Pasal 65 ayat (3) UU Perdagangan.
[234] *Id.*, Pasal 65 ayat (6).

29) Undang-Undang No. 18 Tahun 2014 (UU Kesehatan Jiwa)

Salah satu jenis data yang diatur dalam UU Kesehatan Jiwa adalah data kesehatan jiwa. Dalam UU Kesehatan Jiwa disebutkan bahwa orang yang termasuk sebagai Orang Dengan Masalah Kejiwaan (ODMK) dan Orang Dengan Gangguan Jiwa (ODGJ) berhak mendapatkan informasi yang jujur dan lengkap mengenai data kesehatan jiwanya yang akan diterima dari tenaga kesehatan dengan kompentensi di bidang kesehatan jiwa.[235] Dari rumusan tersebut terlihat bahwa tenaga medis memiliki kewenangan untuk mengakses data privasi, khususnya tentang kesehatan jiwa, dan menyampaikan secara jujur terkait data tersebut.

Meskipun demikian, instrumen ini tidak mengatur jelas bagaimana mekanisme perlindungan dari proses pengumpulan atau pengelolaan data tersebut. Adapun Pasal 75 UU Kesehatan Jiwa hanya menyebutkan bahwa Pemerintah dan Pemerintah Daerah memiliki tugas dan tanggung jawab terhadap penyelenggaraan Upaya Kesehatan Jiwa. Perlindungan terhadap data pribadi terkait kesehatan jiwa seseorang tidak termasuk ke dalam kegiatan penyelenggaraan yang dimaksud.[236] Selain itu, UU Kesehatan Jiwa memungkinkan dibukanya data kesehatan jiwa seseorang guna pemeriksaan atas kepentingan penegakan hukum, baik secara pidana maupun perdata,[237] dan untuk kepentingan pekerjaan atau jabatan tertentu.[238]

30) Undang-Undang No. 36 Tahun 2014 (UU Tenaga Kesehatan)

Tenaga kesehatan yang dalam kegiatannya akan selalu bersinggungan dengan data kesehatan seseorang. Sebagai salah satu bentuk dari jenis data pribadi, maka perlindungan data tersebut harus dilaksanakan. UU Tenaga Kesehatan hanya mengatur bahwa tenaga kesehatan dalam menjalankan praktik memiliki kewajiban untuk menjaga kerahasiaan kesehatan penerima pelayanan kesehatan atau pasien.[239] Hal ini juga diatur dalam Pasal 73 yang secara khusus mengatur tentang rahasia kesehatan penerima pelayanan kesehatan.

Meskipun demikian, dalam Pasal 73 ayat (2) disebutkan bahwa rahasia kesehatan dapat dibuka ke publik untuk kepentingan tertentu, seperti kepentingan penegak hukum dan permintaan pelayanan kesehatan sendiri dan peraturan perundang-undangan lainnya. Namun, secara tegas udnag-undang ini mengatur mekanisme perlindungan data dalam bentuk menjatuhkan sanksi jika terjadi suatu pelanggaran. Pelaku akan diberikan sanksi administratif[240] berupa teguran lisan, peringatan tertulis, denda administratif dan/atau pencabutan izin[241] oleh pemerintah, pemerintah daerah provinsi dan pemerintah daerah kota/kabupaten sesuai dengan kewenangannya.[242]

Dengan beragamnya pengaturan terkait dengan perlindungan data pribadi tersebut, maka melalui tabel di bawah ini dapat ditemukan ringkasan terkait ketentuan yang diatur, serta mekanisme perlindungan data pribadi yang dijamin dalam instrumen yang telah diuraikan sebelumnya. Elaborasi melalui tabel ini dipermudah pula dengan adanya pembagian *cluster* berdasarkan delapan bidang hukum yang menjadi cakupan dari masing-masing regulasi tersebut.

---

[235] Pasal 68(d), 70(1)(e) UU Kesehatan Jiwa.
[236] *Id.*, Pasal 4.
[237] *Id.*, Pasal 71-72.
[238] *Id.*, Pasal 74.
[239] Pasal 58(1)(c) UU Tenaga Kesehatan.
[240] *Id.*, Pasal 82(1).
[241] *Id.*, Pasal 82(4).
[242] *Id.*, Pasal 82(3).

Tabel 3: **Perbandingan Pengaturan terkait Data Pribadi dalam Sejumlah Peraturan Perundang-Undangan di Indonesia**

UNDANG-UNDANG	PENGAKUAN TERHADAP DATA PRIBADI	LIMITASI	MEKANISME PERLINDUNGAN
I. HAM			
KUHP	Pasal 430-434	-	Pasal 430-434
UU HAM	Pasal 29 (1)	Pasal 32	Pasal 76 (1) dan 89 (3)
UU TPPO	Pasal 33	Pasal 29, 32	Pasal 31
II. MEDIA DAN TELEKOMUNIKASI			
UU Telekomunikasi	Pasal 40-42 (1)	Pasal 42 (2), 43	Pasal 56-59
UU ITE	Pasal 26 (1), 31 (1)-(2) dan 43 (2)	Pasal 31 (3) dan 43 (3)	Pasal 26 (2), 38 dan 47
UU KIP	Pasal 6 (3) (c), 17 (g)-(h) dan 19	Pasal 18 (2)	Pasal 23, 26 (1) dan 54
III. PERTAHANAN DAN KEAMANAN			
UU Anti-Terorisme	-	Pasal 30-31	-
UU Intelijen Negara	-	Pasal 31-34	Pasal 15 (1) dan 47
UU Pendanaan Terorisme	Pasal 9 (1)	Pasal 9 (3)	Pasal 9 (2)
IV. PERADILAN			
KUHAP	Pasal 48 (2)-(3)	Pasal 47	Pasal 47 (1)
UU Tipikor	-	Pasal 26, 29, 30	Pasal 31
UU KPK	-	Pasal 12 (a), (c), (f)	Pasal 47 (1)
UU Advokat	Pasal 19 (1)-(2)	Pasal 19 (1)	-
UU KY	Pasal 20A (1) (c)	Pasal 20 (3)-(4)	Pasal 20A (2)
V. KEARSIPAN DAN KEPENDUDUKAN			
UU Adminduk	Pasal 1 (22), 2 (c) dan 84-86	Pasal 87	Pasal 2 (f), 95 dan 98 (2)
UU Kearsipan	Pasal 5, 6 (5), 7 (g), 9, 34-35, 40, 44, 49 (b), 51-52, 66 (2), (5)-(6)	Pasal 66 (1), (3) (i), (7)	Pasal 80 dan 85-86

VI. KESEHATAN			
UU Praktik Kedokteran	Pasal 46, 47, 48 (1) 51 (c) dan 52 (e)	Pasal 48 (2)	Pasal 64, 66-70, 79 dan Bab IX
UU Narkotika	-	Pasal 75 (i), 77-78 dan Pasal 80	-
UU Kesehatan	Pasal 8, 57 (1) dan 189 (2) (c)	Pasal 57 (2)	Pasal 58 (1) dan 182-188
UU Rumah Sakit	Pasal 29 (1) (h), (l), (m), 32 (i), 38 (1) dan 44	Pasal 38 (2)	Pasal 54-55
UU Kesehatan Jiwa	Pasal 68 (d) dan 70 (1) (e)	Pasal 71-72 dan 74	-
UU Tenaga Kesehatan	Pasal 58 (1) (c) dan 70-73 (1)	Pasal 73 (2)	Pasal 82 (1)
VII. KEUANGAN DAN PERBANKAN			
UU Perbankan	Pasal 1 (28), 40 (1)	Pasal 40-44A	Pasal 29 (1), 47 dan 47A
UU BI	-	-	Pasal 24, 27, 34, 35
UU Perbankan Syariah	Pasal 41	Pasal 42-49	Pasal 42 (2), 50, 57, 60, 61
UU TPPU	Pasal 11 (1), 40 (b), 42, 54 (2) dan 83 (1)	Pasal 11 (1), (3), 28, 41 (1) (a), (2), 44 (1) (h), 45, 72	Pasal 11 (2), 72 (5) dan 83 (2)
UU OJK	Pasal 33 (1)-(3)	Pasal 33 (1)-(3)	Pasal 5, 6 (a), 7, 33 (4) dan 52
VIII. PERDAGANGAN DAN PERINDUSTRIAN			
UU Dokumen Perusahan	Pasal 4 dan 11 (3)-(4)	Pasal 11 (5), 18, 19 (2) dan 21	-
UUPK	-	-	-
UU Perdagangan	Pasal 65 (3)	-	Pasal 65 (5)-(6)

Dari paparan tabel diatas menunjukkan bahwa kewenangan mengakses data pribadi dilakukan dalam berbagai macam bidang. Mulai dari bidang HAM, media telekomunikasi, pertahanan dan keamanan, peradilan, kesehatan, kependudukan, perdagangan dan perindustrian, hingga perekonomian termasuk perbankan. Keragaman tersebut berimplikasi pada banyaknya regulasi yang mengatur mekanisme perlindungannya. Tersebarnya regulasi menyebabkan tumpang tindihnya mekanisme dan kewenangan dalam melakukan perlindungan data pribadi itu sendiri.

Setidaknya terdapat 30 regulasi yang mengakui data privasi baik eksplisit maupun implisit dalam peraturan perundang-undangan. Dari peraturan tersebut terdapat beberapa regulasi yang menegaskan bahwa hak atas data pribadi dapat dibatasi untuk kepentingan penegakan hukum dan penerimaan jabatan tertentu. Misalnya dalam KUHAP, polisi diberi kewenangan untuk mengakses surat pribadi yang berkaitan dengan tindak pidana, atau UU Kesehatan yang mengecualikan prinsip kerahasiaan rekam kesehatan pasien hanya untuk kepentingan penegakkan hukum dan pengisian jabatan atau profesi tertentu.

Kewenangan untuk mengawasi pelaksanaan pengelolaan data tanpa memberikan spesifikasi mekanisme perlindungan hanya diatur oleh beberapa regulasi. Pengaturan tersebut juga tidak secara eksplisit menyebutkan kewajiban untuk melindungi data, melainkan hanya sebatas mengawasi proses pengelolaannya. Hanya sebagian regulasi yang mengatur detil mekanisme perlindungan data pribadi dengan cara yang bermacam-macam. Misalnya dalam KUHAP dan UU ITE, kewenangan polisi harus berdasarkan putusan Ketua Pengadilan Negeri. Sedangkan dalam UU TPPU dan UU KPK, kewenangan PPATK dan KPK dalam mengakses data pribadi tidak diharuskan untuk mendapatkan izin ketua Pengadilan terlebih dahulu, melainkan cukup dengan bukti yang cukup dan izin dari ketua lembaga internal.

Dalam keadaan setelah terjadinya pelanggaran perlindungan, beberapa regulasi mengatur sanksi yang berbeda jenis mulai dari ancaman pidana hingga sanksi administratif. Misalnya dalam UU Telekomunikasi dan UU Pendanaan Terorisme, kebocoran perlindungan data dapat diancam pidana penjara. Sedangkan dalam UU Intelejen Negara dan UU KPK penyalahgunaan wewenang penyadapan yang merupakan intervensi hak privasi warga dapat diancam pidana serta pidana denda. Selain ancaman pidana, salah satu mekanisme yang ditawarkan dalam UU Intelejen Negara adalah rehabilitasi atas kerugian yang dialami dari tindakan penyadapan yang diartikan termasuk kegagalan kerahasiaan data.

Tersebarnya pengaturan data pribadi di beberapa regulasi mengakibatkan tumpang tindihnya kewenangan dalam mekanisme perlindungan. Hal ini dapat membuka ruang kesewenang-wenangan pengelolaan dan intervensi data pribadi yang dapat mengakibat kerugian atas pelanggaran hak privasi.

E.3. Perkembangan pembangunan instrumen hukum dalam melindungi data pribadi di Indonesia

Pada perkembangannya instrumen hukum yang melindungi data pribadi secara khusus semakin dibutuhkan. Untuk melengkapi sejumlah peraturan yang tersebar di beberapa undang-undang dan bersifat sangat sektoral, Pemerintah berinisiatif untuk membentuk produk hukum yang mengatur secara khusus mengenai perlindungan data pribadi. Selain itu perlindungan ini tidak lain ditujukan untuk melindungi hak-hak individual di dalam masyarakat sehubungan dengan semakin maraknya pengumpulan, pemrosesan, pengelolaan, dan penyebarluasan data pribadi sebagai konsekuensi perkembangan teknologi. Hal ini juga dibutuhkan untuk memberikan kepercayaan masyarakat dalam memberikan data dan informasi pribadi guna berbagai kepentingan masyarakat yang lebih besar tanpa khawatir akan tindakan penyalahggunaan yang melanggar hak pribadinya.

Hingga saat ini instrumen hukum dalam rangka perlindungan data pribadi masih pada tahap perancangan yang disusun dalam bentuk Rancangan Undang-Undang tentang Perlindungan Data Pribadi (RUU PDP) yang akan masuk dalam Program Legislasi Nasional 2016,[243] dan Rancangan Peraturan Menteri Komunikasi dan Informatikatentang Perlindungan Data Pribadi dalam Sistem Elektronik (RPM PDPSE), yang merupakan turunan dari PP PSTE dan sedianya rampung pada akhir tahun 2015. Selain itu, instrumen lain yang perlu menjadi sorotan adalah Rancangan Kitab Undang-Undang Hukum Acara Pidana (RKUHAP) yang memberikan wewenang kepada penyidik untuk melakukan penyadapan, yang bukan tidak mungkin berpotensi untuk melanggar hak atas privasi seseorang terlanggarkan karena data pribadinya dilacak secara sewenang-wenang tanpa persetujuan pemilik data terlebih dahulu.

1) RUU PDP

Tujuan pembentukan undang-undang ini tidak lain adalah untuk menciptakan sebuah unifikasi perlindungan data pribadi yang tersebar di beberapa peraturan perundang-undangan. Tidak hanya itu, pembuatan RUU PDP juga disinyalir karena tingginya potensi pelanggaran data dan informasi pribadi melalui program Pemerintah, seperti e-KTP, serta maraknya penggunaan jasa transportasi berbasis aplikasi *online*.

Dalam RUU PDP, Pasal 1 mengartikan data pribadi sebagai setiap data yang teridentifikasi dan/atau dapat diidentifikasi, baik secara langsung maupun tidak langsung melalui elektronik atau non elektronik. Selain itu, RUU ini juga menggolongkan jenis data pribadi yang termasuk ke dalam kategori data pribadi sensitif, yakni data atau informasi yang berkaitan dengan agama/keyakinan, kesehatan, kondisi fisik dan kondisi mental, kehidupan seksual, data keuangan pribadi dan data lainnya yang mungkin dapat membahayakan dan merugikan privasi subjek data.

Jaminan perlindungan data pribadi tersebut ditegaskan dalam Pasal 6 RUU PDP yang menyatakan bahwa pengumpulan data pribadi harus dilakukan secara terbatas dan spesifik. Hal ini menyangkut dengan prosedur dalam proses pengumpulan yang harus dengan cara yang sah secara hukum dan adil serta harus berdasarkan pengetahuan dan persetujuan dari orang yang bersangkutan. Lebih jauh, Pasal 10 RUU PDP juga menyebutkan bahwa pada prinsipnya, pengelolaan data pribadi harus dilakukan dengan melindungi keamanan data pribadi dari kehilangan, penyalahgunaan, akses, pengungkapan yang tidak sah, pengubahan atau perusakan data pribadi.

Pada dasarnya pengelolaan data pribadi oleh pihak pengelola harus didasari oleh persetujuan dari subjek atau pemilik data pribadi. Dalam prosesnya, permintaan persetujuan tersebut harus melampirkan informasi mengenai informasi mengenai keijakan pengelola data pribadi dan tujuan pengelolaan data pribadinya. Selain itu juga dijelaskan jenis data apa saja yang akan dikelola serta periode retensi dokumen yang akan diperlihara. Dengan demikian, RUU ini memberikan kewenangan subjek data pribadi untuk menerima, menolak atau menarik kembali persetujuan tersebut. Hal tersebut juga berlaku dalam proses transfer data pribadi pada pihak ketiga, baik dalam lingkup nasional maupun internasional.

[243] Susetyo Dwi Prihadi, "Menkominfo Siap Lindungi Data Pribadi di Dunia Maya", CNN Indonesia, (25 September 2015) <http://www.cnnindonesia.com/teknologi/20150925153941-213-80967/menkominfo-siap-lindungi-data-pribadi-di-dunia-maya/>.

Dalam hal penyelesaian sengketa menyangkut data pribadi, RUU PDP memberikan dua pilihan alternatif, yakni melalui jalur di luar pengadilan dan melalui jalur pengadilan. Adapun pada prosesnya, penyelesaian sengketa pada tahap awal harus melalui luar pengadilan terlebih dahulu, baru kemudian melalui pengadilan apabila pada tahap pertama ini dinyatakan tidak berhasil atau dengan kata lain jalur penyelesaian sengketa melalui pengadilan haruslah dilihat dan digunakan sebagai pilihan akhir (*last resort*).

2) RPM PDPSE

Dalam upaya membentuk suatu jaminan hukum perlindungan data pribadidalam media elektronik, Pemerintah Indonesia, melalui Kementerian Komunikasi dan Informatika RI (Kemenkominfo), sedang menyusun suatu RPMPDPSE sebagai bentuk pelaksanaan ketentuan Pasal 15 ayat (3) PP PSTE. Pada proses pembahasannya, RPM PDPSE ini turut pula mengundang perwakilan dari Ditjen Imigrasi Kementerian Hukum dan HAM RI, ANRI, OJK, Yayasan Lembaga Konsumen Indonesia (YLKI), BI dan Kemenkes RI.[244]

Dalam perkembangannyaRPM ini, mendapatkan kritik dari beberapa pihak, termasuk oleh ELSAM yang menyatakan bahwa perlindungan data pribadi merupakan bagian dari hak atas privasi yang memerlukan legitimasi hukum setingkat Undang-Undang dan bukan melalui Peraturan Menteri.[245] Selain kritik atas model legislasi tersebut, ELSAM juga mencatat empat kelemahan lainnya, yaitu kriteria data pribadi yang dapat diakses oleh penegak hukum, mekanisme pemulihan hak para korban yang data pribadinya terciderai, pengawasan pelaksanaan dari perlindungan data pribadi dalam sistem elektronik, dan terakhir adalah mengenai perlunya perlunya otoritas independen untuk penyelesaian sengketa.[246] Pada akhirnya, Kemenkominfo menyambut baik masukkan ini dan mengakomodirnya ke dalam revisi RPM PDPSE.

3) RKUHAP

Tindakan penyadapan sebagai salah satu pembatasan terhadap hak privasi perlu diatur dalam sebuah produk hukum guna membatasi kewenangan atas tindakan tersebut sekaligus memberikan perlindungan terhadap warga negara. Dalam konteks hukum acara pidana, RKUHAP juga turut mengatur mengenai tindakan penyadapan dalam Pasal 83 dan 84.

Dalam Pasal 83 RKUHAP menunjukkan sebuah mekanisme yang harus ditempuh untuk melakukan penyadapan. Dimana tindakan penyidikan dapat dilaksanakan oleh penyidik setelah mendapatkan izin dari Hakim Komisaris dengan menyertakan alasan pembenar serta mencantumkan durabilitas kewenangan tersebut berlaku.

Dengan adanya rumusan mekanisme penunjukan otoritas yang berwenang atas izin tindakan penyadapan, maka dapat diartikan bahwa ada upaya dalam melakukan perlindungan akan

---

[244] Kementerian Komunikasi dan Informatika RI, "Siaran Pers No.53/PIH/KOMINFO/07/2015 tentang Uji Publik Rancangan Peraturan Menteri mengenai Perlindungan Data Pribadi dalam Sistem Elektronik", (14 Juli 2015) <http://kominfo.go.id/index.php/siaran_pers/detail/5128/Siaran+Pers+No.53-PIH-KOMINFO-07-%202015+tentang+Uji+Publik+Rancangan+Peraturan+Menteri+mengenai+Perlindungan+ Data+Pribadi+dalam+Sistem+%20Elektronik>.

[245] ELSAM, "ELSAM Kritisi Rancangan Peraturan Kementerian Kominfo Tentang Perlindungan Data Pribadi", (31 Juli 2015) <http://elsam.or.id/2015/07/elsam-kritisi-rancangan-peraturan-kementrian-kominfo-tentang-perlindungan-data-pribadi/>.

[246] *Id*.

data pribadi warga negara dalam bentuk pengawasan horizontal berlapis. Mekanisme otoritas tersebut merupakan suatu bentuk pengawasan *pre-facto* atau pengawasan sebelum dilakukannya tindakan intersepsi atau penyadapan. Hal tersebut merupakan salah satu wujud perlindungan dari negara terhadap warganya yang beritikad baik.[247]

F. BENTUK-BENTUK PELANGGARAN TERHADAP KERAHASIAAN DATA PRIBADI

Meskipun sudah diatur dalam berapa peraturan perundang-undangan, pelanggaran terhadap perlindungan data pribadi masih banyak ditemukan, mulai dari praktik penyadapan atau intersepsi secara ilegal hingga kebocoran data pribadi. Fenomena tersebut pada kenyataannya tidak dapat dipisahkan dari massifnya pengumpulan data pribadi dalam skala besar namun tidak diimbangi dengan perlindungan hukum sebagai jaminan hak atas privasi. Akibatnya data pribadi seseorang sangat mudah dipindahtangankan tanpa persetujuan pemiliknya.

Berdasarkan segitiga privasi Kurbalija (2014) yang menguraikan perlindungan hak atas privasi sebagai bagian dari relasi kausa antara individu, negara dan sektor individu, dapat diidentifikasikan sejumlah pola pencideraan terhadap hak atas privasi seseorang.[248] Mulai dari hubungan antara perorangan dengan negara, perorangan dengan sektor industri, hingga hubungan antar-individu itu sendiri yang memungkinkan munculnya resiko pelanggaran terhadap hak atas privasi dari satu individu ke individu lainnya. Khusus untuk konteks peningkaran terhadap hak atas privasi yang dilakukan oleh negara dan sektor industri, sering kali dilakukan dengan metode *surveillance* dengan pola yang dilakukan secara terpisah dan pola yang dilakukan secara bersama-sama.

Praktik pola hubungan antara individu dengan negara atau pemerintah terhadap pelanggaran data pribadi pada prinsipnya terjadilantaran adanya program kerja yang diselenggarakan pemerintah. Dalam konteks ini, beberapa program kerja pemerintah tersebut mengharuskan adanya pengumpulan data pribadi warga negara dalam skala besar (*digital dossier*), seperti program KTP elektronik (e-KTP) dan program*e-health*.

Program e-KTP menghendaki identitas tunggal setiap penduduk agar dapat berlaku seumur hidup.[249] Perekaman data meliputi informasi pribadi warga, termasuk ciri-ciri fisik orang tersebut. Perekaman ciri-ciri fisik ini dilakukan dengan pemindaian terhadap sidik jari dan retina mata, yang digunakan untuk validasi biometrik pemegang KTP. Menurut informasi Kemendagri, hasil dari perekaman data tersebut selanjutnya akan ditanam di dalam e-KTP tersebut.

Titik permasalahan terkait dengan hal ini adalah perihal*server* penyimpan data e-KTP merupakan milik negara lain, sehingga bank data yang dikumpulkan sangat rentan untuk diakses oleh pihak asing dan tidak bertanggungjawab. Selain itu, *vendor* fisik e-KTP ini tidak menganut *open system*, sehingga Kemendagri tidak bisa mengutak-atik sistem tersebut. Bahkan, sebagaimana dilansir oleh Wikileaks, perusahaan Inggris ThorpeGlen menyatakan bahwa melalui e-KTP metode pemindaian sangat mungkin dilakukan.[250] Artinya, dengan

[247] Manthovani, *Op.Cit.*, hal.299.
[248] Jovan Kurbalija, *An Introduction to Internet Governance,* 6th Edition, (Geneva: DiploFoundation, 2014), hal.106-108.
[249] "Apa dan Mengapa e-KTP", (20 Juni 2011) <http://www.e-ktp.com/2011/06/hello-world/>.
[250] Naskah Akademik RUU PDP, *Op.Cit.*, hal.7.

menggunakan perangkat e-KTP warga negara dapat dilacak keberadaan dan aktivitasnya. Dengan demikian, negara dapat mengamati kehidupan pribadi setiap warganya. Hal tersebut tidak lain merupakan pelanggaran semena-mena.

Selain e-KTP, dalam bidang kesehatan misalnya program*e-health* juga memiliki potensi pelanggaran akan hak privasi. Pengumpulan data pasien mencakup rekaman medis masyarakat menjadi sangat penting untuk dilindungi. Hal ini tidak hanya karena akses terhadap rekam medis melanggar privasi, tetapi data tersebut dikhawatirkan dapat dimanfaatkan secara ekonomi oleh penyedia jasa seperti industri obat-obatan atau asuransi. Oleh sebab itu, penting untuk menyediakan regulasi yang menjamin bahwa pihak penyelenggara program maupun pihak pengelola rumah sakit untuk menjaga kerahasiaan data kesehatan pasien yang merupakan data sensitif.

Lebih jauh, tantangan pelanggaran terhadap data pribadi seseorang juga nyatanya dilakukan oleh negara asing. Hal ini dituturkan mantan anggota *National Security Agency* (NSA), Edward Snowden, yang mengungkapkan adanya spionase massal dan pengumpulan data terhadap pelanggan Telkomsel oleh Biro Keamanan dan Komunikasi Selandia Baru (GCSB) bekerja sama dengan mata-mata elektronik Australia (ASD) bersama dengan jaringan spionase *Five Eyes* pada tahun 2009.[251] Pada tahun 2012 upaya penyadapan yang melibatkan peran operator jaringan telekomunikasi kembali terjadi. Kali ini dilakukan oleh NSA bekerja sama dengan intelijen Australia dan melakukan enkripsi terhadap data milik hampir 1,8 juta pelanggan Telkomsel dan Indosat.[252]

Sementara itu, kaitannya dengan pelanggaran terhadap data pribadi individu yang dilakukan oleh pihak swasta atau sektor industri terefleksikan melalui fenomena kebocoran data pribadi. Fenomena seperti ini dapat terlihat dari banyaknya situsyang menawarkan jual-beli data pribadi.[253] Pada tahun 2013, Indonesia dihebohkan dengan munculnya iklan perusahaan yang memiliki 25 juta data pelanggan dan siap diperjualbelikan. Data tersebut pada umumnya dapat diklasifikasi berdasarkan penghasilan, jenis pekerjaan dan rekam deposito yang berkisar ratusan juta. Jenis data yang ditawarkan punbahkan mencakup data nomor ponsel dan alamat lengkap, dan tak jarang catatan transaksi perbankan pelanggan. Hal tersebut diperjualbelikan secara bebas dengan kisaran harga beragam, mulai dari harga seratus ribu hingga jutaan rupiah.[254]

Berdasarkan informasi pelaku pengguna jasa jual-beli data tersebut, transaksi tersebut memiliki istilah *call connection*. Kegiatan tersebut dinilai lazim dalam dunia *marketing* yang menggunakan informasi tersebut untuk menjalankan strategi penawaran berbagai macam produk kepada konsumen. Produk yang ditawarkan mulai dari kartu kredit, asuransi, dan pinjaman uang. Penawaran produk dilakukan melalui kiriman surat elektronik atau melalui telepon. Padahal konsumen sama sekali belum pernah menyerahkan data pribadinya pada

---

[251] Muhaimin, "Snowden: Australia Sadap Indonesia Melalui Telkomsel", Sindo News, (5 Maret 2015) <http://international.sindonews.com/read/972407/40/snowden-australia-sadap-indonesia-melalui-telkomsel-1425529799>

[252] Mariel Grazella, "Minister to Launch New Telkomsel, Indosat Investigation", Jakarta Post, (19 Februari 2014) <http://www.thejakartapost.com/news/2014/02/19/minister-launch-new-telkomsel-indosat-investigation.html>.

[253] Berikut ini adalah beberapa contoh laman yang menjual data pribadi secara bebas <http://www.jualdatabase.org/>; <http://bakulpedia.com/index.php?route=product/product&product_id=139>.

[254] Detik News, "Begini Data Nasabah Diperjualbelikan", (26 Agustus 2013) <http://news.detik.com/berita/2340675/-begini-data-nasabah-diperjualbelikan->.

produsen bersangkutan.[255] Hal ini kenyataannya tidak hanya dilakukan oleh perusahaan swasta, tetapi juga dari institusi pendidikan juga sering dilakukan. Misalnya data pribadi seperti nama, alamat, dan nomor telpon siswa atau mahasiswa diperjual-belikan untuk kepentingan promosi bisnis.

Berkaitan dengan pola pelanggaran data pribadi antar individu, kebocoran data pribadi juga digunakan untuk melaksanakan modus penipuan. Misalnya maraknya penipuan melalui pesan singkat yang meminta pulsa, kecelakaan rekayasa untuk pemerasan, atau undian hadiah fiktif.[256] Keuntungan dari modus penipuan ini disinyalir mencapai enam ratus ribu rupiah (Rp600.000,00) hingga sepuluh juta rupiah (Rp10.000.000,00) perhari.[257] Hal ini bukan hanya mengganggu secara langsung pihak-pihak pemilik data pribadi melainkan merupakan salah satu bentuk pelanggaran hak privasi masyarakat.

Ancaman lain terkait adanya pelanggaran privasi antar-perorangan ini kemudian terjadi pulaseiring dengan semakin meningkatnya penggunaan layanan transportasi berbasis *online*. Dengan menggunakan aplikasi, pemanfaatan transportasi tersebut mengharuskan penumpang memasukkan data pribadi seperti nomor telepon. Karena belum tersedianya mekanisme untuk menghapus data penumpang, maka potensi penyalahgunaan data pribadi oleh pengendara ojek sangat besar. Ditemukan sejumlah kasus terkait pengendara ojek yang melakukan teror penumpang karena telah mendapatkan penilaian buruk atas pelayanan yang diberikannya.[258] Selain itu beberapa penumpang, khususnya perempuan, menyatakan kerap kali diganggu oleh pengendara yang mengirimkan pesan singkat untuk motif pribadi.[259] Sehingga banyak penumpang yang merasa akan kehilangan privasinya dengan belum adanya prosedur khusus dari perusahaan jasa transportasi yang bersangkutan untuk melindungi data pribadi konsumen.

Selain itu pola penyadapan antar-individu juga dapat berupa penyadapan komunikasi dan tindakan pengintaian. Fenomena ini terjadi karena munculnya teknologi alat sadap sederhana dengan menggunakan alat berupa aplikasi atau *software* tertentu mempermudah tindak dapat dilakukan para individu. Salah satunya adalah jasa "*Truth Spy*" yang menggunakan alat *interceraptor* yang dapat menyadap berbagai pembicaraan di ponsel-ponsel yang sinyalnya masih tertangkap di dalam jangkauan alat tersebut. Tidak hanya itu, penyadapan yang dilakukan antar-individu juga dapat dilakukan dengan bantuan perangkat lunak tertentu yang biasa disebut dengan perangkat lunak mata-mata (*spy software* atau*spyware*). Seperti halnya sebuah program jahat semacam *trojan* dan *malware, spyware* mampu melacak aktivitas alat elektronik dan mengirimkan informasi tersebut kepada si penyadap. Program ini juga dapat

---

[255] *Id*.

[256] Egidius Patnistik, "Kebocoran Data Pribadi Gawat", Kompas, (18 Februari 2013) <http://nasional.kompas.com/read/2013/02/18/08161710/Kebocoran.Data.Pribadi.Gawat>.

[257] Detik News, "Polisi Tangkap Komplotan Penipu Melalui SMS dan Internet", (21 April 2014) <http://news.detik.com/berita/2170998/polisi-tangkap-komplotan-penipu-melalui-sms-dan-internet>.

[258] Adityahadi, "Ngerinya Pelanggaran Privasi yang Dilakukan Go-Jek dan GrabBike Terhadap Penumpang Mereka", Aitinesia, (4 September 2015) <http://aitinesia.com/ngerinya-pelanggaran-privasi-yang-dilakukan-go-jek-dan-grabbike-terhadap-penumpang-mereka/>; Jeko Iqbal Reza, "Ojek Online Mulai Ancam Privasi Penumpang?", Liputan 6, (14 September 2015) <http://tekno.liputan6.com/read/ 2317114/ojek-online-mulai-ancam-privasi-penumpang>.

[259] *Id*.

menonaktifkan program tertentu di dalam alat elektronik tersebut, bahkan menghapus informasi yang tersimpan dalam ponsel tanpa sepengetahuan si pemilik.[260]

Dari sejumlah pelanggaran yang terjadi, hingga saat ini belum ada regulasi yang mengatur secara khusus dalam memberikan jaminan perlindungan data pribadi. Selama ini beberapa peraturan perundang-undangan hanya mewajibkan perusahaan untuk melakukan perlindungan secara internal perusahaan, tanpa ada yang menjamin bahwa perusahaan telah melaksakannya. Sehingga ditengah permasalahan pelanggaran hak privasi yang semakin aktual, dan kekosongan hukum yang terjadi, pelanggaran terhadap perlindungan data pribadi akan semakin rentan. Oleh karena itu, pelembagaan mengenai perlindungan data pribadi dalam kerangka hukum Indonesia menjadi penting guna memastikan adanya perbaikan proteksi hak individu secara tepat dan terarah.

G. USULAN PELEMBAGAAN PERLINDUNGAN DATA PRIBADI DI INDONESIA

Seiring dengan maraknya praktik intrusi terhadap data pribadi *vis-à-vis* kewajiban Indonesia dalam menjamin perlindungan hak atas privasi setiap individu, pelembagaan terhadap perlindungan data pribadi ke dalam kerangka hukum Indonesia menjadi mutlak diperlukan. Sebagai upaya untuk menginstitusionalkan hal tersebut, penulis melihat setidaknya dua hal mendasar yang perlu segera dilakukan di Indonesia. ***Pertama***, perlunya dibuat suatu instrumen hukum khusus yang menjamin perlindungan data pribadi. ***Kedua***, pembentukan undang-undang khusus di bidang perlindungan data pribadi perlu pula diiringi dengan didirikannya suatu lembaga khusus yang berwenang untuk mengawasi implementasi terhadap undang-undang tersebut, sehingga dapat memberikan andil terhadap efektivitas perlindungan data pribadi itu sendiri.

G.1. Pembentukan undang-undang tentang perlindungan data pribadi

Meskipun saat ini pengaturan terkait data pribadi sudah termuat dalam 30 peraturan perundang-undangan,[261] pengaturan itu pun masih terlihat sangat bersifat sektoral, sehingga tidak memberikan jaminan perlindungan data pribadi secara menyeluruh. Rendahnya tingkat perlindungan ini tak dapat dipungkiri dipengaruhi oleh besarnya tantangan yang ada dalam merespon massifnya penggunaan data pribadi dewasa ini.

Dalam memahami hal tersebut, tantangan-tantangan tersebut dapat dikategorisasikan ke dalam tigahal pokok, sebagaimana dijabarkan *infra*. Pertama adalah karena terbatasnya dan tumpang tindihnya pengaturan terkini yang mengatur tentang data pribadi. Selain itu, praktik-praktik yang mengganggu kerahasiaan atau keprivasian data seseorang yang cenderung meningkat dewasa ini dapat pula menghambat penikmatan hak atas privasi *per se*. Tantangan berikutnya yang turut mewarnai perlindungan data pribadi Indonesia juga dipengaruhi oleh masih rendahnya kesadaran publik akan pentingnya data milik orang yang bersangkutan tersebut untuk dilindungi.

---

[260] Federal Trade Commission, *Monitoring Software on Your PC: Spyware, Adware, and Other Software*, Laporan Spyware Workshop, (2005) hal.9-10.

[261] Lihat Bagian E.2.

1) Legislasi yang terbatas dan tumpang tindih

Dengan tersegmentasinya pengaturan data pribadi dalam sejumlah undang-undang yang bersifat sektoral. Dampaknya, jaminan perlindungan data pribadi bagi subjek data belum menyeluruh. Dari pemetaan tersebut juga ditemukan beberapa kelemahan daan kekosongan hukum antar-setiap undang-undang tersebut.

Melalui tabel dibawah ini akan terlihat secara lebih jelas perbandingan materi muatan dalam undang-undang tersebut, khususnya terkait dengan pengaturan terhadap (i) pengolahan data, (ii) pembukaan data, dan (iii) mekanisme pertanggungjawaban yang dapat diterapkan sekiranya terjadi pelanggaran. Penetapan terhadap ketiga indikator yang digunakan untuk mengklasifikasikan perundang-undangan ini sesungguhnya merupakan inti sari dari prinsip-prinsip terbaik yang berlaku di Uni Eropa, OECD dan APEC. Tidak hanya itu, penggunaan parameter ini menjadi pentingkarena hal tersebut sejalan dengan pandangan HRC dalam Komentar Umum 16 ICCPR yang menekankan bahwa ketiga indikator tersebut di atas sebagai hal yang harus termuat dalam suatu legislasi.[262] Harapannya, melalui tabel ini dapat terurai titik kekurangan dan ketumpang-tindihan regulasi yang dimiliki oleh Indonesia.

Tabel 4: **Perbandingan Prinsip Pengolahan, Pembukaan Data dan Akuntabilitas**

UNDANG-UNDANG	A. PENGOLAHAN DATA				B. PEMBUKAAN DATA			C. AKUNTABILITAS	
	A1	A2	A3	A4	B1	B2	B3	C1	C2
I. HAM									
KUHP	-	-	-	-	-	-	-	✓	-
UU HAM	✓	-	-	-	✓	✓	-	-	-
UU TPPO	-	-	-	-	✓	✓	✓	-	-
II. MEDIA DAN TELEKOMUNIKASI									
UU Telekomunikasi	✓	✓	-	-	✓	-	-	✓	-
UU ITE	-	✓	-	-	✓	-	-	✓	✓
UU KIP	-	-	-	-	✓	✓	-	✓	-
III. PERTAHANAN DAN KEAMANAN									
UU Anti-Terorisme	-	-	-	-	✓	✓	✓	-	-
UU Intelijen Negara	-	-	-	-	✓	✓	✓	✓	✓
UU Pendanaan Terorisme	✓	-	-	-	✓	-	-	✓	-
IV. PERADILAN									
KUHAP	-	-	-	-	✓	✓	-	-	-
UU Tipikor	-	-	-	-	✓	✓	-	-	-
UU KPK	-	-	-	-	✓	✓	-	-	-
UU Advokat	✓	-	-	-	✓	-	-	-	-

[262] UN Doc.CCPR/C/GC/16 (1994) para.10.

UU KY	-	-	-	-	✓	✓	-	✓	-
V. KEARSIPAN DAN KEPENDUDUKAN									
UU Adminduk	✓	-	-	✓	✓	-	-	✓	✓
UU Kearsipan	✓	-	✓	✓	✓	✓	✓	✓	-
VI. KESEHATAN									
UU Praktik Kedokteran	✓	✓	✓	-	✓	✓	-	✓	-
UU Narkotika	-	-	-	-	✓	✓	✓	-	-
UU Kesehatan	✓	✓	-	-	✓	✓	-	-	✓
UU Rumah Sakit	✓	-	-	-	✓	✓	✓	✓	-
UU Kesehatan Jiwa	✓	✓	-	-	✓	-	-	-	-
UU Tenaga Kesehatan	✓	✓	-	-	✓	✓	-	✓	-
VII. KEUANGAN DAN PERBANKAN									
UU Perbankan	✓	✓	-	-	✓	✓	-	✓	-
UU BI	-	-	-	-	-	-	-	-	-
UU Perbankan Syariah	✓	✓	-	-	✓	✓	-	✓	✓
UU TPPU	✓	-	-	-	✓	✓	-	-	-
UU OJK	✓	-	-	-	✓	-	-	✓	-
VIII. PERDAGANGAN DAN PERINDUSTRIAN									
UU Dokumen Perusahaan	✓	-	✓	✓	✓	-	-	-	-
UUPK	-	-	-	-	-	-	-	-	-
UU Perdagangan	-	✓	-	-	✓	-	-	✓	✓

Keterangan:
A1 : Tujuan pengolahan data pribadi
A2 : Notifikasi atau persetujuan dari pemilik data pribadi
A3 : Rentan waktu retensi data pribadi
A4 : Penghancuran, penghapusan atau pengubahan data pribadi
B1 : Tujuan pembukaan data pribadi kepada pihak ketiga
B2 : Pemberi izin untukmembuka data pribadi kepada pihak ketiga
B3 : Jangka waktu data pribadi dapat dibuka kepada pihak ketiga
C1 : Sanksi bagi pelanggar perlindungan data pribadi
C2 : Mekanisme pemulihan bagi korban yang hak privasinya terlanggarkan

Melalui tabel ini terlihat bahwa tidak ada satu regulasi pun yang mampu mengatur kesemua indikator yang idealnya eksis untuk memperkuat jaminan perlindungan data pribadi. Misalnya, KUHP, UU Telekomunikasi, UU ITE, UU Adminduk, UU Kearsipan, UU Kesehatan, UU Rumah Sakit, UU Perbankan dan UU Perbankan Syariah memuat ketentuan sanksi bagi pelanggar data pribadi, sedangkan ada pula undang-undang lain yang tidak memuat ketentuan sanksi seperti itu. Tidak hanya itu, meskipun KUHAP dan UU ITE memungkinkan dilakukannya penyadapan atau intersepsi terhadap data pribadi, ironisnya hal ini tidak

didukung dengan adanya pengaturan khusus terhadap mekanisme atas praktik tersebut, sebagaimana diamanahkan oleh Mahkamah Konstitusi.[263]

Kelemahan lain dari undang-undang yang telah dimiliki oleh Indonesia saat ini juga nampak dari masih minimnya jumlah undang-undang yang memberikan jaminan pemulihan bagi korban yang hak atas privasinya terlanggarkan. Tercatat setidaknya UU Intelijen Negara dan UU Kesehatan yang mengakui adanya jaminan pemulihan bagi korban yang data pribadinya tersadapkan oleh pihak ketiga.

Bahkan, lebih parah lagi ditemukan sebuah undang-undang yang sejatinya memuat ketentuan tentang data privasi, namun pengaturannya malah tidak ada sedikit pun, seperti terlihat dalam UUPK. Pada intinya, hal ini justru semakin memperkuat kenyataan bahwa ketentuan perundang-undangan yang telah hidup di Indonesia saat ini masih bersifat terbatas dan belum mampu melindungi penikmatan data pribadi secara seutuhnya.

Dalam hal pengaturan yang bersifat tumpang tindih. Sama halnya dengan praktik di Amerika Serikat, kelemahan terkait dengan perlindungan data pribadi di Indonesia terjadi karena ketidakseragaman pengertian data pribadi itu sendiri, sebagai konsekuensi dari tersebarnya pengaturan dari hal tersebut. Hingga saat ini, Indonesia belum memiliki definisi yang solid mengenai data pribadi, setiap undang-undang memiliki pengertian sendiri mengenai data pribadi sesuai dengan bidang pengaturannya. Misalnya, dalam UU Adminduk dan PP PSTE mendefinisikan data pribadi secara umum, sebagai data perseorangan tertentu yang disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiannya. Akan tetapi, dalam undang-undang lainnya, *inter alia*, UU Perbankan, UU Perbankan Syariah dan UU Telekomunikasi definisi data pribadi spesifik ditujukan bagi keterangan nasabah penyimpan dan simpanannya serta nasabah investor dan investasinya, dan catatan/rekaman pemakaian jasa telekomunikasi. Perbedaan konsep mengenai data pribadi ini tentu akan berpengaruh pada tingkat pengamanan atas data itu sendiri.

Ketidaksesuaian pengaturan antar-sesama perundang-undangan yang berlaku ini juga terlihat dalam hal penyadapan terhadap data pribadi. Beberapa undang-undang, seperti UU Narkotika, UU Terorisme dan UU Intelijen Negara, memerlukan persetujuan dari otoritas yang berwenang sebelum melakukan intersepsi; sementara dalam UU KPK hal tersebut tidak diperlukan. Ketumpang-tindihan regulasi ini juga bahkan diperparah dengan tidak adanya kesamaan rentan waktu yang dimungkinkan dalam melakukan praktik penyadapan tersebut. UU Narkotika misalnya hanya mengizinkan sampai tiga bulan dan dapat diperpanjang kembali sampai tiga bulan sesudahnya, sedangkan UU KPK tidak memiliki limitasi waktu untuk melakukan penyadapan itu. Oleh karena itu, dengan tidak samanya pengaturan antara ketiga puluh instrumen yang ada ini, hal ini dapat pula membahayakan upaya perlindungan data pribadi.

3) Meningkatnya intrusi data pribadi

Dalam negara yang demokratis, interaksi yang konstan dalam mengartikulasikan pendapat publik dan proses legislatif tak jarang dapat menimbulkan ketegangan antara norma hukum dan sosial, sehingga sangat tidak mungkin hukum dibuat bermusuhan atau bertentangan dengan kehendak masyarakat. Namun demikian, hukum yang dibuat tersebut harus juga

[263] Lihat Putusan MK No. 5/PUU-VIII/2010 (2010).

mampu merespon gelombang pasang kebiasaan sosial yang tak tertahankan itu.[264] Artinya, hukum yang dibuat oleh pemerintah dapat menjadi agen perubahan sekaligus kontrol terhadap kehidupan sosial bermasyarakat.

Dewasa ini, potensi pelanggaran data dan informasi pribadi di Indonesia cenderung meningkat. Melalui dari lahirnya program Pemerintah, seperti e-KTP hingga *e-health*, sampai maraknya penyalahgunaan data pribadi konsumen jasa transportasi berbasis aplikasi *online*.[265] Dengan keterbatasan regulasi yang ada, hal ini kemudian berimplikasi pada lemahnya pemulihan bagi korban yang hak-haknya terlanggarkan tersebut. Hal inilah yang kemudian menjadi landasan mendesak dirumuskannya RUU PDP,[266] dengan harapan agar rancangan undang-undang yang terbaru itu dapat memberikan pengaruh dalam mengontrol perilaku sosial masyarakat Indonesia terhadap perlindungan data pribadi orang lain.

4) Rendahnya kesadaran publik

Urgensitas akan perlindungan data pribadi di Indonesia saat ini nyatanya tidak berbanding lurus dengan pemahaman publik akan pentingnya data tersebut untuk dilindungi. Hal ini pun nyatanya diakui oleh akademisi,[267] serta bukti riil bahwa masih rendahnya pengajuan kasus di pengadilan terkait dengan gangguan atas keprivasian datang seseorang, terlepas dari 30 undang-undang yang sudah ada dan memiliki pengaturan yang bersinggungan dengan perlindungan terhadap data pribadi.

Dalam rangka menjawab kelemahan-kelemahan dalam hukum positif Indonesia sekarang ini, serta dengan mempertimbangkan strategi yang diterapkan di Jepang saat ini dalam memberikan jaminan perlindungan data pribadi yang lebih esensial. Oleh karena itu, diperlukan suatu bentuk undang-undang khusus yang ditujukan untuk memberikan kepastian hukum dalam perlindungan data pribadi. Urgensitas pembentukan undang-undang yang secara khusus mengatur perlindungan data pribadi, sebagai suatu *cross-cutting issue*, sesungguhnya harus dilihat sebagai bentuk komitmen Indonesia terhadap seruan Majelis Umum PBB kepada semua negara anggotanya, termasuk Indonesia, untuk meninjau kembali legislasi-legislasi yang telah dibuat dan berkaitan dengan perlindungan data pribadi itu tetap menjunjung tinggi nilai-nilai hak atas privasi berdasarkan standar hukum HAM internasional.[268]

Lagi pula, seiring dengan meningkatnya tren transaksi perdagangan internasional, jaminan perlindungan data pribadi menjadi mutlak diperlukan bagi pelaku usaha dalam melakukan bisnis internasional. Sehingga sebagai konsekuensinya, Indonesia, sebagai negara anggota APEC, didorong untuk mampu meningkatkan jaminan perlindungan data pribadi demi terciptanya kerja sama ekonomi internasional yang lebih baik. Dengan demikian, semakin memadainya perlindungan data pribadi di Indonesia, maka akan meningkatkan pula kans transaksi perdagangan internasional.

---

[264] W. Friedmann, *Law in a Changing Society*, (Berkeley: University of California Press, 1959) hal.10.

[265] Penjelasan lebih lanjut mengenai keanekaragaman [potensi] intrusi terhadap data pribadi di Indonesia dapat dilihat pada tulisan ini dalam Bagian F; lihat pula survei terkait intrusi terhadap data pribadi seseorang yang dilakukan di kota Bandung dalam Naskah Akademik RUU PDP, *Op.Cit.*, hal.4.

[266] Anggara, et al., *Menyeimbangkan Hak: Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia*, (Jakarta: ICJR, 2015) hal.1-2.

[267] Imam Santoso, "Kominfo: Indonesia perlu UU perlindungan data pribadi", Antara News, (16 April 2013) <http://www.antaranews.com/berita/369399/kominfo-indonesia-perlu-uu-perlindungan-data-pribadi>.

[268] Resolusi 68/167, *Op.Cit.*, para.4(b)-(c).

G.2. Pendirian badan pengawasan tentang perlindungan data pribadi

Sebagai upaya untuk merealisasikan perlindungan data pribadi, pendirian suatu institusi pengawasan yang independen menjadi hal yang tak terelakan lagi. Sehubungan dengan hal tersebut, independensi dalam konteks ini harus dipahami pula sebagai terbebas dari segala macam campur tangan pemerintah.[269] Praktik-praktik di dunia pun bahkan menunjukkan pentingnya pengawasan data pribadi melalui institusi independen.[270]

Khusus untuk konteks Indonesia, berdasarkan sejumlah instrumen hukum nasional yang telah dikaji di atas,[271] nyatanya tidak semua instrumen tersebut menyediakan klausula ketentuan yang secara khusus memandatkan institusi tertentu sebagai badan yang berwenang untuk melakukan pemantauan terhadap penggunaan dan penyalahgunaan data pribadi. Tabel di bawah ini menunjukkan perbandingan di antara ketiga puluh undang-undang tersebut terkait dengan pencantuman ketentuan tentang badan pengawas yang berwenang untuk mengawasi pengelolaan data pribadi seseorang, mulai dari proses perekaman, pengolahan, penyimpanan, penggunaan, sampai dengan menerima pengaduan jika ada pelanggaran.

Tabel 5: **Perbandingan Institusi Pengawas Berdasarkan Peraturan Perundang-Undangan yang Berlaku di Indonesia**

UNDANG-UNDANG	INSTITUSI PENGAWAS
I. HAM	
KUHP	-
UU HAM	Komnas HAM
UU TPPO	-
II. MEDIA DAN TELEKOMUNIKASI	
UU Telekomunikasi	Badan Regulasi Telekomunikasi Indonesia (BRTI)[272]
UU ITE	Menteri Komunikasi dan Informasi RI[273]
UU KIP	Komisi Informasi[274]
III. PERTAHANAN DAN KEAMANAN	
UU Anti-Terorisme	(i) Atasan Penyidik; (ii) Kepala Kepolisian Daerah; (iii) Kepala Kejaksaan Tinggi; (iv) Ketua Pengadilan Negeri; dan (v) Majelis Hakim Ketua
UU Intelijen Negara	(i) Kepala BIN; dan (ii) Komite Pengawas Intelijen Negara (Sub-Komisi 1 DPR RI)[275]
UU Pendanaan Terorisme	(i) Lembaga Pengawas dan Pengatur (LPP); (ii) PPATK;

[269] UN Doc.A/HRC/27/37 (2014) para.37.
[270] Lihat Tabel 2 "Perbandingan Perlindungan Data Pribadi di Beberapa Negara".
[271] Lihat Bagian E.2.
[272] Ditetapkan berdasarkan Keputusan Menteri Perhubungan No. 31 Tahun 2003 tentang Penetapan Badan Regulasi Telekomunikasi Indonesia.
[273] Lihat Pasal 33 ayat (1) *jo.* Pasal 15 dan 4 huruf (e) PP PSTE; Pasal 35 RPM PDP.
[274] Lihat Pasal 36-37 PerKIP No. 1 Tahun 2010.
[275] Lihat Pasal 43 ayat (2)-(3) UU Intelijen Negara.

	(iii) Direktorat Jendral Bea Cukai; dan (iv) Pengadilan Negeri
IV. PERADILAN	
KUHAP	Ketua Pengadilan Negeri
UU KPK	(i) Ketua KPK; dan (ii) Hakim Pengadilan Tindak Pidana Korupsi
UU Advokat	Majelis Kehormatan Advokat[276]
UU Tipikor	(i) Ketua KPK; dan (ii) Hakim Pengadilan Tindak Pidana Korupsi
UU KY	-
V. KEARSIPAN DAN KEPENDUDUKAN	
UU Adminduk	Menteri Dalam Negeri RI[277]
UU Kearsipan	(i) Tim Pengawas Kearsipan Eksternal; dan (ii) Tim Pengawas Kearsipan Internal
VI. KESEHATAN	
UU Praktik Kedokteran	(i) Kementerian Kesehatan RI; (ii) Konsil Kedokteran Indonesia; dan (iii) Dinas Kesehatan
UU Narkotika	BNN
UU Kesehatan	Menteri Kesehatan RI
UU Rumah Sakit	(i) Kepala Dinas Kesehatan Provinsi; (ii) Kepala Dinas Kesehatan Kabupaten/Kota; dan (iii) Organisasi profesi terkait[278]
UU Kesehatan Jiwa	-
UU Tenaga Kesehatan	(i) Presiden RI; (ii) Pemerintah Daerah; (iii) Konsil Tenaga Kesehatan Indonesia; dan (iv) Organisasi profesi terkait[279]
VII. KEUANGAN DAN PERBANKAN	
UU Perbankan	BI[280]
UU BI	BI
UU Perbankan Syariah	BI[281]
UU TPPU	(i) Kepala Kepolisian RI; (ii) Pimpinan instansi atau lembaga atau komisi terkait; (iii) Jaksa Agung RI; dan (iv) Majelis Hakim Ketua
UU OJK	OJK[282]

[276] Lihat Pasal 12-13 UU Advokat (Kewenangan pendirian Komisi Pengawas ditentukan oleh Organisasi Advokat).

[277] Lihat lebih lanjut dalam Pasal 51-52 Peraturan Pemerintah Nomor 37 Tahun 2007 tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan; Peraturan Menteri Dalam Negeri Nomor 25 Tahun 2011 tentang Pedoman Pengkajian, Pengembangan dan Pengelolaan Sistem Informasi Administrasi Kependudukan.

[278] Lihat pula Pasal 16 ayat (1) Permenkes Rekam Medis.

[279] Lihat Pasal 80 UU Tenaga Kesehatan.

[280] Keberadaan kewenangan ini selanjutnya diganti oleh OJK.

[281] *Id*.

[282] Lihat pula Pasal 51-52 POJK No. 1/POJK.07/2013; SEOJK No. 14/SEOJK.07/2014.

VIII. PERDAGANGAN DAN PERINDUSTRIAN	
UU Dokumen Perusahaan	-
UUPK	-
UU Perdagangan	(i) Menteri Perdagangan RI; (ii) Pemerintah Daerah;[283] (iii) Komite Perdagangan Nasional;[284] dan (iv) Menteri Komunikasi dan Informasi RI[285]

Jika kita mengacu kepada lembaga-lembaga yang telah disebutkan di atas, maka nampak jelas bahwa walaupun ketiga puluh undang-undang tersebut mengulas atau setidak-tidaknya memiliki ketentuan yang bersinggungan dengan perlindungan data pribadi, termasuk aspek intrusi terhadap data pribadi. Ironisnya, hal ini tidak diikuti dengan penyediaan lembaga yang berwenang untuk mengawasi praktik intrusi tersebut. Setidaknya tercatat tiga undang-undang tersebut tidak mendelegasikan kewenangan supervisi tersebut kepada instansi tertentu.

Kelemahan lain dari regulasi yang telah eksis, kaitannya dengan kelembagaan penegakan perlindungan data pribadi di Indonesia, tercermin dari kenyataan bahwa meskipun beberapa undang-undang telah menunjuk instansi-instansi independen yang secara khusus memiliki kewenangan untuk melakukan pengawasan – baik secara langsung maupun tidak langsung – terhadap perlindungan data pribadi, *inter alia*, Komnas HAM, Komisi Informasi, BRTI, OJK, Majelis Kehormatan Advokat, Komite Perdagangan Nasional dan Konsil Tenaga Kesehatan Indonesia. Akan tetapi, semua lembaga independen ini merupakan subordinat pemerintah, artinya lembaga ini sepenuhnya berada di bawah kekuasaan pemerintah.

Sebagai ilustrasi, walaupun Pasal 1 ayat (1) UU OJK mendeskripsikan OJK sebagai lembaga independen yang berwenang melakukan pengawasan terhadap data pribadi nasabah bank. Nyatanya, sesuai dengan amar putusan Mahkamah Konstitusi dalam uji materiil UU OJK,[286] penggunaan kata "independen" ini tidak secara serta merta menegasi kedudukan OJK sebagai penyelenggara negara, mengingat adanya unsur-unsur perwakilan pemerintah di dalam struktur kelembagaan OJK. Pula, adanya koordinasi, kerjasama dan harmonisasi kebijakan dengan lembaga-lembaga pemerintah lain semakin menunjukkan eksistensi OJK sebagai bagian dari pemerintah.[287] Sehingga, dapat disimpulkan bahwa OJK merupakan lembaga pemerintah.
Merujuk kepada pendelegasian kewenangan pengawasan terhadap perlindungan data pribadi kepada instansi pemerintahan sebagaimana disinggung di atas. Praktik seperti ini jelas bertentangan dengan standar internasional yang menekankan pentingnya suatu institusi independen [tanpa campur tangan pemerintah seutuhnya] yang dapat mensupervisi segala macam bentuk tindakan yang melibatkan penggunaan data pribadi.[288]

Permasalahan lain yang juga timbul terkait dengan eksistensi semua lembaga ini adalah realita bahwa masing-masing badan ini bertindak hanya sebatas kepada isu-isu sektoral yang dimuat dalam undang-undang sektoral yang bersangkutan semata, dan tidak didukung dengan

[283] Lihat Pasal 98 UU Perdagangan.
[284] *Id.*, Pasal 97(4)(e).
[285] Mengikuti ketentuan yang ada dalam UU ITE.
[286] Lihat Putusan MK No. 25/PUU-XII/2014 (2014).
[287] *Id.*, para.3.17.1.
[288] UN Doc.A/HRC/17/27 (2011) para.58; UN Doc.CCPR/C/GC/16 (1994) para.10.

kewenangan supervisi yang lintas batas isu. Kekosongan mekanisme seperti ini tentu akan menimbulkan problematika di masa depan, apabila terjadi suatu intrusi terhadap data pribadi.

Lebih jauh, kelemahan lain dari mekanisme pengawasan terhadap perlindungan data pribadi di Indonesia adalah tidak adanya keseragaman mekanisme dalam melakukan pengawasan antar-instansi tersebut, membuat upaya perlindungan data pribadi dalam semua sektor kehidupan menjadi tidak merata satu sama lain.

Menilik kepada *status quo* mekanisme penegakan hukum yang diharapkan dapat memberikan jaminan perlindungan bagi data pribadi yang cenderung menunjukkan kekurangannya tersebut, maka pendirian suatu lembaga pengawasan data pribadi menjadi agenda yang tak terelakan lagi dalam membumikan perlindungan data pribadi pada kerangka hukum Indonesiayang lebih konkrit. Sehingga, melalui badan khusus yang memiliki kewenangan untuk melakukan supervisi terhadap semua bentuk data pribadi tersebut diharapkan untuk tidak hanya mampu mengatasi kesenjangan-kesenjangan tersebut, tetapi menjadi langkah awal bagi perbaikan mekanisme perlindungan data pribadi ke depannya.

H. PENUTUP

Realitas hari ini memperlihatkan adanya praktik pertukaran dan peredaran data yang bersifat lintas batas (*cross border*). Pada sisi lain, terdapat konsep hak atas privasi yang telah lahir sejak lama dan diakui sebagai hak fundamental setiap individu. Berdasarkan fenomena tersebut maka diperlukan sebuah integrasi terkait hak privasi yang menjadi norma dalam melakukan perlindungan terhadap data pribadi yang sejalan dengan perkembangan inovasi teknologi. Kebutuhan transformasi perlindungan ditujukan untuk menciptakan sebuah pengaturan objektif guna menciptakan keseimbangan antara privasi, keamanan dan lalu lintas peredaran data. Hal tersebut yang kemudian mendorong entitas internasional dalam melahirkan pengakuan untuk meningkatkan perlindungan atas hak atas privasi melalui instrumen HAM internasional. Termasuk dalam konteks Indonesia, urgensi pengaturan untuk memberikan perlindungan data pribadi secara menyeluruh menjadi penting mengingat pengaturan perlindungan hak atas privasi warga masih tersebar dan berdiaspora dalam berbagai pengaturan sektoral.

Oleh karenanya, pemerintah dan DPR harus segera mengambil inisiatif pembahasan suatu undang-undang, yang secara spesifik memuat ketentuan perihal perlindungan data pribadi, sesuai dengan standar hukum HAM internasional. Selain itu, melihat luasnya cakupan perlindungan data pribadi, termasuk entitas yang melakukan pengumpulan dan penyimpanan data (pemerintah dan swasta), penting untuk mendorong pendirian suatu badan independen yang secara khusus memiliki wewenang untuk melakukan supervisi pengimplementasian undang-undang tersebut secara efektif.

***

DAFTAR PUSTAKA

BUKU

Anggara, et al., *Menyeimbangkan Hak: Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia*, (Jakarta: ICJR, 2015).

Beynon-Davies, P., *Information Systems: An Introduction to Informatics in Organisations*, (Basingstoke: Palgrave Macmillan, 2002).

Bu, Yuanshi (ed.), *Chinese Civil Law*, (Munchen: C.H. Beck, 2013).

CoE dan ECtHR, *Handbook on European Data Protection Law*, (Luxembourg: EU, 2014).

De Hert, Paul dan Papakonstantinou, Vagelis, *The Data Protection Regime in China: In-depth Analysis for the LIBE Committee*, (Brussels: European Union, 2015).

Delahaie, Henri dan Paoletti, Félix, *Informatique et Libertés*, (Paris: Editions La Découverte, 1987).

Djoni S. Gazali dan Rachmadi Usman, *Hukum Perbankan*, (Jakarta: Sinar Grafika, 2010).

Edmon Makarim, *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*, (Jakarta: PT. RajaGrafindo Persada, 2005).

Friedmann, W., *Law in a Changing Society*, (Berkeley: University of California Press, 1959).

Fuster, Gloria González, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, (Heidelberg: Springer, 2014).

Gardner, Bryan A. (ed.), *Black's Law Dictionary*, 8th Edition, (St. Paul: West Pub. Co., 2004).

Greenleaf, Graham, *Asian Data Privacy Laws: Trade and Human Rights Perspectives*, (Oxford: Oxford University Press, 2014).

Hondius, F.W. dan Hondius, F.W., *Emerging Data Protection in Europe*, (Amsterdam: North-Holland Pub. Co., 1975).

Kurbalija, Jovan, *An Introduction to Internet Governance,* 6th Edition, (Geneva: Diplo Foundation, 2014).

Liu, Nancy Yue, *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics*, (Oxon: Routledge, 2012).

Mayer-Schönberg, Viktor, "Generational development of data protection in Europe", dalam Philip E. Agre dan Marc Rotenberg (eds.), *Technology and Privacy: The New Landscape*, (Cambridge: MIT Press, 1997).

Miller, Arthur R., *The Assault on Privacy: Computers, Data Banks, and Dossiers*, (Ann Arbor: University of Michigan Press, 1971).

Ministry of Justice, Sweden (Regeringskansliet), *Personal Data Protection: Information on the Personal Data Act*, 4th edition, (Stockholm: Fritzes kundtjänst, 2006).

Nowak, Manfred, *U.N. Covenant on Civil and Political Rights CCPR Commentary*, 2nd rev. Ed., (Kehl: N.P. Engel Verlag, 2005).

Purwanto, *Penelitian tentang Perlindungan Hukum Data Digital*, (Jakarta: BPHN Departemen Hukum dan HAM, 2007).

Reda Manthovani, *Penyadapan vs. Privasi*, (Jakarta: Bhuana Ilmu Populer, 2013).

Shinta Dewi Rosadi, *CyberLaw: Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasional*, (Bandung: Widya Padjadjaran, 2009).

Smedinghoff, Thomas J. (ed.), *Online Law: The SPA's Legal Guide to Doing Business on the Internet*, (Reading: Addison-Wesley Developers Press, 1996).

Wahyudi Djafar dan Asep Komarudin, Perlindungan Hak Atas Privasi di Internet: Beberapa Penjelasan Kunci, (Jakarta: ELSAM, 2014).

Westin, Alan F., *Privacy and Freedom*, (London: Atheneum, 1967).

ARTIKEL, JURNAL, MAKALAH DAN LAPORAN

Burchell, J., "The Legal Protection of Privacy in South Africa: A Transplantable Hybrid", 13 *J. Comp. L.* 1 (2009).

Burkert, Herbert, "Privacy/Data Protection: A German/European Perspective", pada *Proceedings of 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council, Wood Hole, Massachusets*, (1999).

Federal Trade Commission, *Monitoring Software on Your PC: Spyware, Adware, and Other Software*, Laporan Spyware Workshop, (2005).

Greenleaf, Graham, "Five Years of the APEC Privacy Framework: Failure or Promise?", 25 *Computer L. & Security Rep.* 28, (2009).

Greenleaf, Graham, "Malaysia: ASEAN's first data privacy Act 2010 in force", 126 *Privacy L. & Bus. Int'l Rep.* 11 (2013).

Greenleaf, Graham, "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories", 23 *J.L.I.S.* 1, (2014).

Livingston, Scott dan Greenleaf, Graham, "Whys and wherefores – illegal provision under Chinese law", 131 *Privacy L. & Bus. Int'l Rep.* 1 (2014).

Marnia Rani, "Perlindungan Otoritas Jasa Keuangan terhadap Kerahasiaan dan Keamanan Data Pribadi Nasabah Bank", 2 *Jurnal Selat* 1, (2014).v

Palupy, Heppy Endah, *Privacy and Data Protection: Indonesia Legal Framework*, Tesis Program Master Law and Technology di Universiteit van Tilburg, Tilburg (2011).

Riccardi, J. Lee, "The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?", 6 *B.C. Int'l & Comp. L. Rev.* 1 (1983).

Schwartz, Paul M. dan Solove, Daniel J., "Reconciling Personal Information in the United States and European Union", 102 *Calif. L. Rev.* 877 (2014).

Schwartz, Paul M. dan Solove, Daniel J., "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", 86 *N.Y.U. L. Rev.* 1814, (2011).

Steele, Jonathan, "Data Protection: An Opening Door? The Relationship Between Accessibility and Privacy in Sweden in an EU perspective", 24 *Liverpool L. Rev.* 19 (2002).

Warren, Samuel dan Brandeis, Louis D., "The Right to Privacy", 4 *Harv. L. Rev.* 5 (1890).

INSTRUMEN INTERNASIONAL

- *American Convention on Human Rights*, 1144 UNTS 123, 22 November 1969.
- *APEC Privacy Framework*, (2004).
- *ASEAN Human Rights Declaration*, 18 November 2012.
- *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, E.T.S. No.108, 28 Januari 1981.
- *Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, O.J. L. 281, 23 November 1995.
- *Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector*, O.J. L. 24, 30 Januari 1998.
- *Directive 2002/58/EC on Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, O.J. L. 201, 31 Juli 2002.
- HRC, *General Comment 16: Right to Privacy (Art.17)*, UN Doc.CCPR/C/GC/16 (1994).

- HRC, *General Comment 27: Freedom of Movement (Art.12)*, UN Doc.CCPR/C/21/Rev.1/Add.9 (1999).
- HRC, *General Comment 31: Nature of the General Legal Obligation on States Parties to the Covenant*, UN Doc.CCPR/C/21/Rev.1/Add.13 (2004).
- *International Covenant on Civil and Political Rights*, 999 UNTS 171, 16 Desember 1966.
- La Rue, Frank, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc.A/HRC/17/27 (2011).
- La Rue, Frank, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc.A/HRC/23/40 (2013).
- *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, (1980).
- OHCHR, *The right to privacy in the digital age*, Report, UN Doc.A/HRC/27/37 (2014).
- *The right to privacy in the digital age*, Resolusi Dewan HAM 28/16, UN Doc.A/HRC/RES/28/16 (2015).
- *The right to privacy in the digital age*, Resolusi Majelis Umum 68/167, UN Doc.A/RES/68/167 (2014).
- *Universal Declaration of Human Rights*, UN Doc.217/A (III) (1948).

PERATURAN PERUNDANG-UNDANGAN NEGARA LAIN

- Afrika Selatan, *National Credit Act*, No. 34/2005.
- Afrika Selatan, *Proclamation by the President of the Republic of South Africa*, No. R. 25 2014, (17 April 2014) <http://www.gov.za/sites/www.gov.za/files/37544_rg10173_pro25.pdf>.
- Afrika Selatan, *Promotion of Access to Information Act*, No.2/2000, (2 Februari 2000) <http:// www.dfa.gov.za/department/accessinfo_act.pdf>.
- Afrika Selatan, *Protection of Personal Information Act*, No.4/2013, (26 November 2013) <http:// www.justice.gov.za/legislation/acts/2013-004.pdf>.
- Afrika Selatan, *Regulation of Interception of Communications and Provision of Communication-Related Information Act*, No. 70/2002.
- Amerika Serikat, *Privacy Act*, 5 U.S.C. 552a, (31 Desember 1974) <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf>.
- Filipina, *Data Privacy Act*, No.10173, (15 Agustus 2012) <http://www.gov.ph/2012/08/15/republic -act-no-10173/>.
- Inggris, *Data Protection Act*, (16 Juli 1998) <http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf>.
- Jepang, *Act on the Protection of Personal Information*, No. 57, (30 Mei 2003) <http://www.cas. go.jp/jp/seisaku/hourei/data/APPI.pdf>.
- Jepang, *Amendment Act on the Protection of Personal Information*, (9 September 2015) <http:// www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf>.
- Jepang, *Cabinet Order for the enforcement of the Act on the Protection of Personal Information*, No.507, (10 Desember 2003) <http://www.worldlii.org/int/other/PrivLRes/2003/2.html>.
- Jepang, *Financial Service Agency (FSA) Privacy Guidelines*, (20 November 2009).
- Jepang, *Ministry of Economy, Trade and Industry (METI) Guidelines*, No. 2, (9 Oktober 2009).
- Jepang, *Ministry of Labour, Health and Welfare (MLHW) Guidelines for Medical and Nursing Enterprises*, (24 Desember 2004).

- Jerman, *Federal Data Protection Act (Bundesdatenschutzgesetz)*, (27 Januari 1977) <http://www.gesetze-im-internet.de/englisch_bdsg/>.
- Malaysia, *Penal Code (Amendment) Act 2012*, No.574, (31 Juli 2012) <http://www.vertic.org/media/National%20Legislation/Malaysia/MY_Criminal_Code_2013.pdf>.
- Malaysia, *Personal Data Protection Act*, No.709, (2 Juni 2010) <http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf>.
- Prancis, *Law on Computers, Files and Freedoms (Loi relative à L'informatique, aux Fichiers et aux Libertés)*, No.78-17, (6 Januari 1978) <https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf>.
- Swedia, *Data Act (Datalag)*, SFS 1973:289, (11 Mei 1973).
- Swedia, *Penal Code*, SFS 1962:700, (1962) <http://www.government.se/contentassets/5315d2707 6c9420198 28d6c36521696e/swedish-penal-code.pdf>.
- Swedia, *Personal Data Act*, SFS 1998:204, (29 April 1998).
- RRT, *Constitution*, (1982).
- RRT, *Criminal Law*, (1 Juli 1979) <http://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm>.
- RRT, *General Principles of Civil Law*, (1986).
- RRT, *MIIT Guidelines for Personal Information Protection within Public and Commercial Services Information Systems*, (21 Januari 2013).
- RRT, *MIIT Regulations on Standarizing Market Order for Internet Information Services*, (7 Desember 2011).
- RRT, *MIIT Telecommunications and Internet Personal User Data Protection Regulations*, (28 Juni 2013).
- RRT, *SC-NPC Decision on Internet Information Protection*, (2012) <https://chinacopyrightand media.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/>.
- RRT, *Tort Liability Law*, (2009).

PERATURAN PERUNDANG-UNDANGAN INDONESIA

- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Undang-Undang No. 1 Tahun 1946 tentang Kitab Undang-Undang Hukum Pidana.
- Undang-Undang No. 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana.
- Undang-Undang No. 8 Tahun 1997 tentang Dokumen Perusahaan.
- Undang-Undang No. 10 Tahun 1998 tentang Perbankan.
- Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen.
- Undang-Undang No. 23 Tahun 1999 tentang Bank Indonesia.
- Undang-Undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi.
- Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi.
- Undang-Undang No. 39 Tahun 1999 tentang Hak Asasi Manusia.
- Undang-Undang No. 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi.
- Undang-Undang No. 15 Tahun 2003 tentang Penetapan Perppu No. 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme.
- Undang-Undang No. 18 Tahun 2003 tentang Advokat.
- Undang-Undang No. 29 Tahun 2004 tentang Praktik Kedokteran.

- Undang-Undang No. 23 Tahun 2006 tentang Administrasi Kependudukan.
- Undang-Undang No. 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang.
- Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik.
- Undang-Undang No. 21 Tahun 2008 tentang Perbankan Syariah.
- Undang-Undang No. 35 Tahun 2009 tentang Narkotika.
- Undang-Undang No. 36 Tahun 2009 tentang Kesehatan.
- Undang-Undang No. 43 Tahun 2009 tentang Kearsipan.
- Undang-UndangNo.44Tahun2009tentangRumahSakit.
- Undang-Undang No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.
- Undang-Undang No. 17 Tahun 2011 tentang Intelijen Negara.
- Undang-Undang No. 18 Tahun 2011 tentang Perubahan Undang-Undang No. 22 Tahun2004 tentang Komisi Yudisial.
- Undang-Undang No. 21 Tahun 2011 tentang Otoritas Jasa Keuangan.
- Undang-Undang No. 9 Tahun 2013 tentang Pencegahan dan Pemberantasan TindakPidana Pendanaan Terorisme.
- Undang-Undang No. 7 Tahun 2014 tentang Perdagangan.
- Undang-Undang No. 18 Tahun 2014 tentang Kesehatan Jiwa.
- Undang-Undang No. 36 Tahun 2014 tentang Tenaga Kesehatan.
- Peraturan Presiden No. 67 Tahun 2011 tentang Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional.
- Peraturan Pemerintah No. 37 Tahun 2007 tentang Pelaksanaan Undang-Undang No. 23 Tahun 2006 tentang Administrasi Kependudukan.
- Peraturan Pemerintah No. 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi.
- Peraturan Pemerintah No. 37 Tahun 2007 tentang Pelaksanaan UU Adminduk.
- Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
- Peraturan Pemerintah No. 43 Tahun 2015 tentang Pihak Pelapor dalam Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.
- Peraturan Menteri Dalam Negeri No. 25 Tahun 2011 tentang Pedoman Pengkajian, Pengembangan dan Pengelolaan Sistem Informasi Administrasi Kependudukan.
- Peraturan Menteri Kesehatan No. 269/Menkes/Per/III/2008 tentang Rekam Medis.
- Peraturan Menteri Kesehatan No. 1171/Menkes/Per/VI/2011 tentang Sistem Informasi Rumah Sakit.
- Peraturan Menteri Kesehatan No. 36 Tahun 2012 tentang Rahasia Kedokteran.
- Peraturan Menteri Kesehatan No. 55 Tahun 2013 tentang Penyelenggaraan Pekerjaan Rekam Medis.
- Keputusan Menteri Perhubungan No. 31 Tahun 2003 tentang Penetapan Badan Regulasi Telekomunikasi Indonesia.
- Peraturan Bank Indonesia No. 2/19/PBI/2000 tentang Persyaratan dan Tata Cara Pemberian Perintah atau Izin Tertulis Membuka Rahasia Bank.
- Peraturan Kepala Arsip Nasional Republik Indonesia No. 38 Tahun 2015 tentang Pedoman Pengawasan Kearsipan.
- Peraturan Komisi Informasi Publik No. 1 Tahun 2010 tentang Standar Layanan Informasi Publik.

- Peraturan Otoritas Jasa Keuangan No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan.
- Surat Edaran Otoritas Jasa Keuangan No. 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen.

YURISPRUDENSI

- *Census Act (Volkszählung)*, BVerfGE 65, 1, Mahkamah Konstitusi Jerman (1983).
- *Hannover v. Germany*, No.59320/00, Eur.Ct.H.R. (2004).
- *Leander v. Sweden*, No.9248/81, Eur.Ct.H.R. (1987).
- *MK v. France*, No.19522/09, Eur.Ct.H.R. (2013).
- Putusan No. 5/PUU-VIII/2010, Mahkamah Konstitusi RI (2010).
- Putusan No. 25/PUU-XII/2014 Mahkamah Konstitusi RI (2014).
- *Shanghai Roadway*, Putusan Tahun 2012, Pengadilan Distrik Zhabei, Shanghai, RRT.
- *European Commission v. Federal Repulic of Germany*, C-518/07, Ct.J.E.U. (2010).
- *European Commission v. Repulic of Austria*, C-614/10, Ct.J.E.U. (2012).
- *Weber and Saravia v. Germany*, No.54934/00, Eur.Ct.H.R. (2006).
- *Zhou Jianping*, Putusan No. 612 Tahun 2009, Pengadilan Distrik Xiangzhou, Zhuhai, RRT.

SUMBER INTERNET DAN LAINNYA

"Apa dan Mengapa e-KTP", (20 Juni 2011) <http://www.e-ktp.com/2011/06/hello-world/>.

"Speech by the Deputy Minister of Justice and Constitutional Development, the Hon JH Jeffery, MP, during the Debate on Vote 21: Justice and Constitutional Development, National Assembly", (19 Mei 2015) <http://www.justice.gov.za/m_speeches/2015/20150519_BudgetVoteDM.html>.

Adityahadi, "Ngerinya Pelanggaran Privasi yang Dilakukan Go-Jek dan GrabBike Terhadap Penumpang Mereka", Aitinesia, (4 September 2015) <http://aitinesia.com/ngerinya-pelanggaran-privasi-yang-dilakukan-go-jek-dan-grabbike-terhadap-penumpang-mereka/>.

Audi Eka Prasetyo, "Apa yang Harus Go-Jek dan *Startup* Transportasi Lainnya Lakukan untuk Melindungi Privasi Pengguna", Tech in Asia, (15 September 2015) <https://id.techinasia. com/talk/privasi-pengguna-go-jek/>.

Bambang Pratama, "Perlindungan Data Pribadi pada Pemesanan Transportasi Online Sejenis Go-Jek", Rubrik Universitas Bina Nusantara (Agustus 2015) <http://business-law.binus. ac.id/2015/09/12/perlindungan-data-pribadi-pada-pemesanan-transportasi-online-sejenis-go-jek/>.

BBC, *First Data Protection Act fines issued by commissioner*, (24 November 2010) <http://www.bbc.com/news/uk-11821203>.

Chu, Kathy, "Dun & Bradstreet Fined, Four Sentenced in China", Wall Street Journal, (9 Januari 2013)<http://www.wsj.com/articles/SB10001424127887323482504578230781008932240>.

Daniel Gunawan, "Pengguna Go-Jek Diteror Setelah memberikan *Bad Review*!", Tech in Asia, (3 September 2015) <https://id.techinasia.com/talk/pengguna-go-jek-diteror-setelah-memberikan-bad-review/>.

Detik News, "Begini Data Nasabah Diperjualbelikan", (26 Agustus 2013) <http://news.detik.com/berita/2340675/-begini-data-nasabah-diperjualbelikan->.

Detik News, "Polisi Tangkap Komplotan Penipu Melalui SMS dan Internet", (21 April 2014) <http://news.detik.com/berita/2170998/polisi-tangkap-komplotan-penipu-melalui-sms-dan-internet>.

Direktorat Jenderal IKP, Kementerian Komunikasi dan Informasi, dan Cyberlaw Centre Fakultas Hukum, Universitas Padjadjaran Bandung, *Naskah Akademik Rancangan Undang-Undang tentang Perlindungan Data Pribadi*, (2014).

Egidius Patnistik, "Kebocoran Data Pribadi Gawat", Kompas, (18 Februari 2013) <http://nasional.kompas.com/read/2013/02/18/08161710/Kebocoran.Data.Pribadi.Gawat>.

ELSAM, "ELSAM Kritisi Rancangan Peraturan Kementerian Kominfo Tentang Perlindungan Data Pribadi", (31 Juli 2015) <http://elsam.or.id/2015/07/elsam-kritisi-rancangan-peraturan-kementrian-kominfo-tentang-perlindungan-data-pribadi/>.

Imam Santoso, "Kominfo: Indonesia perlu UU perlindungan data pribadi", Antara News, (16 April 2013) <http://www.antaranews.com/berita/369399/kominfo-indonesia-perlu-uu-perlindungan-data-pribadi>.

Jeko Iqbal Reza, "Ojek Online Mulai Ancam Privasi Penumpang?", Liputan 6, (14 September 2015) <http://tekno.liputan6.com/read/2317114/ojek-online-mulai-ancam-privasi-penumpang>.

Kementerian Komunikasi dan Informatika RI, "Siaran Pers No.53/PIH/KOMINFO/07/2015 tentang Uji Publik Rancangan Peraturan Menteri mengenai Perlindungan Data Pribadi dalam Sistem Elektronik", (14 Juli 2015) <http://kominfo.go.id/index.php/siaran_pers/ detail/5128/Siaran+Pers+No.53-PIH-KOMINFO-07%202015+tentang+Uji+Publik+Rancangan+Peraturan+Menteri+mengenai+Perlindungan+Data+Pribadi+dalam+Sistem+%20Elektronik>.

Mariel Grazella, "Minister to Launch New Telkomsel, Indosat Investigation", Jakarta Post, (19 Februari 2014) <http://www.thejakartapost.com/news/2014/02/19/minister-launch-new-telkomsel-indosat-investigation.html>.

Michalsons, "Information Regulator in South Africa", (20 November 2015) <http://www.michalsons.co.za/blog/information-regulator-in-south-africa/13893>.

Muhaimin, "Snowden: Australia Sadap Indonesia Melalui Telkomsel", Sindo News, (5 Maret 2015)<http://international.sindonews.com/read/972407/40/snowden-australia-sadap-indonesia-melalui-telkomsel-1425529799>.

Roebuck, John C., et al, "Japan: Amendment of the Personal Information Protection Act", Jones Day, (4 November 2015) <http://www.mondaq.com/x/440786/Data+Protection+Privacy/Amendment+of+the+Personal+Information>.

Susetyo Dwi Prihadi, "Menkominfo Siap Lindungi Data Pribadi di Dunia Maya", CNN Indonesia, (25 September 2015) <http://www.cnnindonesia.com/teknologi/20150925153 941-213-80967/menkominfo-siap-lindungi-data-pribadi-di-dunia-maya/>.

Umeda, Sayuri, "Online Privacy Law: Japan", Library of Congress, (Juni 2002) <https://www.loc.gov/law/help/online-privacy-law/japan.php#_ftn10>.

Yoga Hastyadi Widiartanto, "Indonesia Belum Punya UU Perlindungan Data Pribadi", Kompas, (17 Februari 2015)<http://tekno.kompas.com/read/2015/02/17/09544927/indonesia.belum.punya.uu.perlindungan.data.pribadi>.

PROFIL ELSAM

Lembaga Studi dan Advokasi Masyarakat *(Institute for Policy Research and Advocacy*), disingkat ELSAM, adalah organisasi advokasi kebijakan, berbentuk Perkumpulan, yang berdiri sejak Agustus 1993 di Jakarta. Tujuannya adalah turut berpartisipasi dalam usaha menumbuh-kembangkan, memajukan dan melindungi hak-hak sipil dan politik, serta hak-hak asasi manusia pada umumnya – sebagaimana diamanatkan oleh Konstitusi UUD 1945 dan Deklarasi Universal Hak Asasi Manusia Perserikatan Bangsa-Bangsa 1948. Sejak awal, semangat perjuangan ELSAM adalah membangun tatanan politik demokratis di Indonesia melalui pemberdayaan masyarakat sipil lewat advokasi dan promosi hak asasi manusia (HAM).

Kegiatan utama ELSAM adalah: (1) studi kebijakan dan hukum yang berdampak pada hak asasi manusia; (2) advokasi hak asasi manusia dalam berbagai bentuknya; (3) pendidikan dan pelatihan hak asasi manusia; dan (4) penerbitan dan penyebaran informasi hak asasi manusia.

Program kerja ELSAM yaitu: (1) pengintegrasian prinsip dan norma hak asasi manusia dalam kebijakan dan hukum negara; (2) pengintegrasian prinsip dan norma hak asasi manusia dalam kebijakan tentang operasi korporasi yang berhubungan dengan masyarakat lokal; dan (3) penguatan kapasitas masyarakat sipil dalam memajukan hak asasi manusia.

Alamat:

Jl. Siaga II No.31, Pejaten Barat, Pasar Minggu
Jakarta-INDONESIA 12510
Tel. +62 21 7972662, 79192564, Fax. +62 21 79192519
Surel: office@elsam.or.id, laman: www.elsam.or.id
Twitter: @elsamnews - @ElsamLibrary

PANCASILA

KETUHANAN YANG MAHA ESA

KEMANUSIAAN YANG ADIL DAN BERADAB

PERSATUAN INDONESIA

KERAKYATAN YANG DIPIMPIN OLEH HIKMAT KEBIJAK-SANAAN DALAM PERMUSYAWARATAN / PERWAKILAN

KEADILAN SOSIAL BAGI SELURUH RAKYAT INDONESIA

ELSAM
LEMBAGA STUDI & ADVOKASI MASYARAKAT

ELSAM
LEMBAGA STUDI & ADVOKASI MASYARAKAT